



⑬ **BUNDESREPUBLIK
DEUTSCHLAND**



**DEUTSCHES
PATENTAMT**

⑫ **Übersetzung der
europäischen Patentschrift**

⑧ **EP 0 619 565 B 1**

⑩ **DE 37 52 138 T 2**

⑤ Int. Cl.⁶:
G 07 B 17/00
G 07 F 7/10
G 07 F 17/26

② Deutsches Aktenzeichen: 37 52 138.1
⑥ Europäisches Aktenzeichen: 94 101 534.9
⑥ Europäischer Anmeldetag: 1. 9. 87
⑧ Erstveröffentlichung durch das EPA: 12. 10. 94
⑧ Veröffentlichungstag
der Patenterteilung beim EPA: 5. 11. 97
④ Veröffentlichungstag im Patentblatt: 26. 3. 98

③ Unionspriorität:

903379 02. 09. 86 US
935244 26. 11. 86 US

⑦ Patentinhaber:

Pitney Bowes, Inc., Stamford, Conn., US

⑦ Vertreter:

HOFFMANN · EITLE, 81925 München

⑧ Benannte Vertragstaaten:

AT, BE, CH, DE, FR, GB, IT, LI, LU, NL, SE

⑦ Erfinder:

WRIGHT, Christopher B., San Francisco, CA 94115,
US; BRISTOW, Stephen, Los Altos Hills, CA 94022,
US

⑤ Automatisiertes Transaktionssystem mit einsteckbaren Karten zum Fernladen von Gebühren oder Dienstprogrammdateien

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patentamt inhaltlich nicht geprüft.

DE 37 52 138 T 2

DE 37 52 138 T 2

27.11.97

27. Nov. 1997

EP Nr. 94 101 534.9-2209

61 901 s1/bn

Die Erfindung betrifft ein automatisiertes Transaktionssystem, das eine Benutzerkarte mit einem Mikroprozessor zum Ausführen von sicheren Transaktionen, in dem ein Wertartikel von einer Station ausgegeben wird, und ein in dem Speicher der Karte gespeicherter Kontostand belastet wird. Insbesondere wird die Erfindung auf ein PortoTransaktionssystem angewendet, in dem ein Portokonto innerhalb des Mikroprozessors der Karte aufrecht erhalten wird, und für Transaktionen mit Portodruck- und Zumeßstationen benutzt wird.

EP-A-0 137 737 offenbart ein auf einem Mikroprozessor basierendes Postverarbeitungssystem, das ein Diskettenlaufwerk zum Einführen einer Diskette durch einen Benutzer hat, einen Prozessor zum Ausführen von Systemfunktionen, einschließlich der Funktion des Abwickelns von Portobeträgen durch das System, und eine Tastatur, die mit dem Prozessor verbunden ist, um einem Benutzer zu ermöglichen eine Anfrage für ein abzuwickelndes Porto einzugeben. Eine Mehrzahl von Disketten ist bereitgestellt, wobei jede Diskette Gebühreninformation speichert, die einer entsprechenden der Mehrzahl von verschiedenen durch das System abzuwickelnden Portodiensten entspricht, das auch Verbindungsleitungen umfaßt zum Herstellen einer Verbindung zwischen seinem Prozessor und dem die Diskette aufnehmenden Diskettenlaufwerk. Der Betriebsprozessor umfaßt ein gespeichertes Programm zum Ausführen einer Gebührenberechnungsprozedur zum Berechnen des Portowerts eines verlangten Artikels, unter Benutzung der in dem Speicher der Diskette gespeicherten Gebühreninformation, und ein Wertdrucker ist bereitgestellt ist zum Drucken eines verlangten Portobetrages in Übereinstimmung mit dem durch den Betriebsprozessor berechneten Portowerts.

Verkaufsstellenstationen (POS) und automatisierte Ausgabemaschinen (ATM) sind in großem Maße in Verbindung mit verschiedenen Kartentypen, die für Verkauf- oder Kredittransaktionen an Benutzer ausgestellt werden, benutzt worden. Beispielsweise geben Banken regelmäßig Kontokarten aus, die eine auf einem Streifen gespeicherte magnetisch codierte Nummer haben, um auf das Konto des Benutzers über ATM-Stationen zuzugreifen. Kreditkarten, die codierte magnetische Streifen haben, werden in ATM- oder POS-Stationen eingeführt, um auf ein zentrales Kontosystem zur Autorisierung einer Kredittransaktion zuzugreifen. Es hat auch Vorschläge gegeben, Karten zu

benutzen, die große nichtflüchtige Speicher haben, z.B. magnetische, integrierte Schaltkreise (IC) oder optische Speicher zum Speichern und Abrufen von benutzerspezifischer Information, wie beispielsweise eine medizinische Vorgeschichte, biographische Geschichte, Aufrechterhaltung von Kontostand und Transaktionsvergangenheit, etc..

Diese herkömmlichen Systeme verwenden im allgemeinen eine Karte, die einen passiven Speicher hat, der in einem Kartenleser oder einer durch einen Verkäufer instandgehaltenen elektronischen Station gelesen wird. Die Sicherheit der Karten ist problematisch, da die meisten herkömmlich benutzten Karten passiv sind, und sich selbst oder die spezielle Transaktionen, für die sie verwendet werden, nicht bestätigen. Stattdessen wird ein direkter (On-Line)-Zugriff über eine Station auf ein zentrales Kontosystem, wie beispielsweise Bank- oder Kreditkartenkontenaufzeichnungen, benötigt, um jede Transaktion zu bestätigen. Diese Notwendigkeit legt einem Verkäufer, wie beispielsweise Bankfilialen und Einzelhandelsgeschäften, die die Stationeneinrichtungen instandhalten müssen, sowie dem Bediener des zentralen Kontosystems, das ausreichenden On-Line-Zugang für alle Benutzer des Systems bereitstellen muß und die Sicherheit des gesamten Systems gewährleisten muß, eine zusätzliche Zeit- und Kostenlast auf.

Im Vergleich, Off-Line-Transaktionen, z.B. zwischen einem Benutzer mit einer autorisierten Karte und einer Station, die nicht mit dem zentralen Kontosystem verbunden ist, haben den Nachteil, daß der Verkäufer nicht jede Transaktion bestätigen muß. Ein Karteninhaber führt nur die Karte in eine Station ein, um für einen Kauf zu bezahlen, und die autorisierte Summe der Karte wird mit der Summe der Transaktion belastet. In Off-Line-Transaktionen kann die Verantwortung des Verkäufers reduziert, und der Transaktionsvorgang vereinfacht werden, so daß eine Transaktion durch den Gebrauch von weitverbreiteten Benutzerkarten und automatischen Stationen komplett automatisiert werden kann.

Jedoch sind Off-Line-Transaktionen anfälliger auf den Gebrauch von gefälschten Karten und auf Manipulation der Stationen. Somit müssen die Karten sicher gemacht werden und die Transaktionen auf kleine Summen limitiert werden. Als ein Beispiel für herkömmliche Kartensicherheitsmaßnahmen kann eine Speicherkarte in eine Anzahl von getrennt gültig zu machender Abschnitte mit limitiertem Wert unterteilt werden, die irreversibel mit jeder Transaktion belastet werden, wie in den US-Patenten 4,204,113 und 4,256,955 von Giraud et al. offenbart. Eine persönliche Identifikationsnummer (PIN) kann zum Zeitpunkt des Ausstellens

in den Speicher der Karte geschrieben werden und bei jeder Transaktion von dem Benutzer verlangt werden. Die Stationen werden normalerweise dadurch sicher gemacht, daß sie in Bereichen unterhalten werden, zu welchen der Zugang begrenzt oder beaufsichtigt ist. Jedoch erhöhen diese Anforderungen die Betriebskosten des Systems und vermindern gleichzeitig seine Nützlichkeit.

Die Raffiniertheit des Kartenfälschens und Kreditbetrugs hat mit dem weitverbreiteten Gebrauch von Konto- und Kreditkarten zugenommen, und noch größere Sicherheitsmaßnahmen werden momentan gebraucht, um die Gültigkeit von Kartentransaktionen zu versichern. Herkömmliche Mikroprozessorkarten verwenden lokale Programme zur Kontrolle des Zugriffs der auf der Karte gespeicherten Daten, Speichern eine ausgewählte Benutzer-PIN, um einen autorisierten Benutzer zu bestätigen, und Verhindern den Gebrauch der Karte, wenn ein nicht autorisierter Benutzer erfaßt wird, wie beispielsweise nach einer limitierten Anzahl von nicht korrekten PIN-Eingaben. Obwohl solche Mikroprozessorkarten höhere Sicherheit als passive Karten liefern, das die gesamte System weiterhin anfällig dahingehend, daß wenn einmal eine gültige Benutzer-PIN festgestellt worden ist, eine gestohlene Karte für nicht autorisierte Transaktionen in jeder Station benutzt werden kann, und die Stationen selber einer Durchdringung unterworfen sind. Diese Anfälligkeiten können durch Limitieren der Anzahl autorisierter Karten ausgeglichen werden, durch kontrollierten Zugriff zu den Stationen, oder durch das Benötigen direkter Bestätigung der Transaktion. Jedoch erhöhen solche Maßnahmen wieder die Kosten des Systems und verringern dessen Nützlichkeit.

Ein potentieller Anwendungsbereich von automatisierten Systemen, die Konto- oder Kreditkarten verwenden, ist in Portoverkaufs- und -Zumeßmaschinen. Käufe von Porto- und Versandtransaktionen erfolgen hauptsächlich persönlich mit Bargeld über Schalter an Postämtern. Nur eine limitierte Art von Portobriefmarken kann von öffentlichen Verkaufsmaschinen erworben werden. Die meisten privaten Portozumeßmaschinen haben limitierte Betriebseigenschaften, und deren Zumeßvorrichtungen müssen periodisch entfernt werden, und vom Postamt aufgefüllt zu werden. Die Größe und das Gewicht der Zumeßvorrichtungen machen diese unbequem zu tragen. Einige Zumeßsysteme können durch einen entfernt gelegenen Computer aufgefüllt werden, aber der Anrufer muß immer noch die Kontozentrale anrufen und die Anweisungen des Bedieners manuell an der Frankiermaschine ausführen.

Die Eliminierung von Bargeldkäufen, persönlichen Versandtransaktionen, unnötiger Limitierung von automatisierten Postdiensten und körperlichem Nachfüllen von Portozumeßmaschinen könnte in hohem Maße die Warteschlangen in Postämtern reduzieren und die weitere Verbreiterung von Portoverkaufs- und -zumeßmaschinen zur Zweckmäßigkeit für Benutzer erleichtern, und einen größeren Zugriff auf Postdienste bereitstellen. Der Gebrauch von Konto- oder Kreditkarten für automatisierte postalische Maschinen ist in Betracht gezogen worden. Jedoch würden die Sicherheitsprobleme von herkömmlichen kartenautomatisierten Systemen verlangen, daß Benutzerkarten nur für eine relativ kleine vorbezahlte Portosumme für gültig erklärt werden, daß Verkauf- und -zumeßmaschinen eine limitierte Zahl postalischer Produkte bereitstellt und mit einer limitierten Gesamtportosumme aufgefüllt werden, und daß ein Zugriff auf die Maschinen streng kontrolliert wird. Diese Einschränkungen sind ein wesentliches Hindernis, das zur Schwierigkeit einer Implementierung eines automatisierten postalischen Transaktionssystems beiträgt.

In Anbetracht der voranstehenden Nachteile und Probleme von herkömmlichen Systemen ist es eine Hauptaufgabe der Erfindung ein automatisierte Transaktionssystem bereitzustellen, das Sicherheitsmerkmale hat, die den weitverbreiteten Gebrauch von Konto- oder Kreditkarten für Off-Line-Transaktionen und die Verbreitung von automatisierten Transaktionsstationen, zu denen ein Zugriff nicht streng kontrolliert werden muß, erleichtern werden. Insbesondere wird erwünscht, daß die Karte und der Station zusammenarbeiten, um simultan ein Ausgeben eines Wertes durch die Station und ein Belasten eines autorisierten Guthabens durch die Karte auszuführen.

Gemäß einem Aspekt der Erfindung ist ein automatisiertes Transaktionssystem bereitgestellt, das eine Transaktionsstation mit einem Aufnahmeschlitz umfaßt, um darin eine tragbare Benutzerkarte durch einen Benutzer einzuführen, einen Betriebsabschnitt in der Station zum Ausführen von Stationsfunktionen, einschließlich der Funktion einer Transaktion eines Wertartikels durch die Station, und eine Eingabevorrichtung, die mit der Station verbunden ist, um einem Benutzer die Eingabe einer Nachfrage für ein durch die Station abzuwickelnden Wertartikels zu ermöglichen, worin: eine Anzahl von tragbaren Gebührenkarten bereitgestellt ist, jede Gebührenkarte einen Speicher darin eingebettet hat zum Speichern von Gebühreninformation, die einer entsprechenden der Mehrzahl von verschiedenen durch die Station abzuwickelnden Transaktionsdiensten

entspricht, und eine Datenausgabevorrichtung mit dem Speicher verbunden ist; ein zweiter Aufnahmeschlitz ist in der Station bereitgestellt, zur Aufnahme der Gebührenkarten; die Station umfaßt Verbindungsleitungen zum Herstellen einer Verbindung zwischen ihrem Betriebsabschnitt und der Datenausgabevorrichtung einer in den zweiten Aufnahmeschlitz der Station eingeführten Gebührenkarte; der Betriebsabschnitt der Station umfaßt ein gespeichertes Programm zum Ausführen einer Überprüfungsprozedur zum Überprüfen, daß eine durch den Benutzer eingeführte Gebührenkarte einem ausgewählten Transaktionsdienst entspricht, für den ein Wertartikel verlangt wird, und eine Gebührenberechnungsprozedur zum Berechnen des Transaktionsdienstwerts eines verlangten Artikels, unter Verwendung der in dem Speicher der eingeführten Gebührenkarte gespeicherten Gebühreninformation; und ein Wertausgabeabschnitt ist mit der Station bereitgestellt zur Ausgabe eines verlangten Artikels des ausgewählten Transaktionsdienstes in Übereinstimmung mit dem Überweisungsdienst-Wert, der in der Gebührenberechnungsprozedur berechnet wurde, die durch den Betriebsabschnitt der Station ausgeführt wurde, die betreibbar ist zu veranlassen, daß der Transaktionsdienst-Wert auf der Benutzerkarte aufgezeichnet wird.

Gemäß eines anderen Aspekts der Erfindung ist ein automatisiertes Transaktionssystem bereitgestellt, die einen Transaktionsstation mit einem Aufnahmeschlitz umfaßt, um darin eine tragbare Benutzerkarte durch einen Benutzer einzuführen, und einen Betriebsabschnitt in der Station zur Ausführung von Stationsfunktionen, einschließlich der Funktion einer Transaktion eines Wertartikels durch die Station, wobei: eine Vielzahl von tragbaren Dienstkarten bereitgestellt ist, jede Dienstkarte darin einen Speicher zum Speichern von Dienstprogramminformationen eingebettet hat, die einem entsprechenden der Vielzahl von verschiedenen durch die Station auszuführenden Diensten entspricht, und eine Datenausgabevorrichtung, die mit dem Speicher verbunden ist; ein zweiter Aufnahmeschlitz ist in der Station zur Aufnahme der Dienstkarten bereitgestellt; die Station umfaßt Verbindungsleitungen zum Herstellen einer Verbindung zwischen ihrem Betriebsabschnitt und der Datenausgabevorrichtung einer in den zweiten Aufnahmeschlitz der Station eingeführten Dienstkarte; der Betriebsabschnitt der Station umfaßt ein gespeichertes Programm zur Ausführung einer Bestätigungsprozedur zum Bestätigen, daß eine durch den Benutzer eingeführte Dienstkarte einem ausgewählten Transaktionsdienst entspricht, für die ein Wertartikel verlangt wird, und eine

Leistungsprogrammbenutzungsprozedur zum Benutzen des in dem Speicher der eingeführten Dienstkarte gespeicherten Transaktionsdiensts-Programms; und ein Wertausgabeabschnitt ist mit der Station bereitgestellt, zur Ausgabe eines verlangten Artikels des ausgewählten Transaktionsdienstes in Übereinstimmung mit dem von dem Betriebsabschnitt der Station benutzten Transaktionsdiensts-Programm, der ferner betreibbar ist, den Transaktionsdiensts-Wert zu berechnen und veranlaßt, daß er auf der Benutzerkarte aufgezeichnet wird.

Die oben genannten Prinzipien, Vorteile und Kennzeichen der Erfindung werden anschließend im einzelnen in Verbindung mit den folgenden Abbildungen beschrieben, in denen zeigt:

Fig. 1 schematisch eine bevorzugte Ausführungsform einer automatisierten postalischen Transaktionsstation, die gemäß der Erfindung eine Mikroprozessorkarte benutzt;

Fig. 2a eine Struktur in der Ausführungsform von Fig. 1, zum Ausführen einer sicheren Handshake-Erkennungsprozedur zwischen der Mikroprozessorkarte und einem Wertausgabeabschnitt der Station, und

Fig. 2b die Handshake-Folge skizziert;

Fig. 3 die von dem System der Fig. 1 bereitgestellten mehrfachen Sicherheitsstufen;

Fig. 4 eine andere Ausführungsform der postalischen Transaktionsstation der Erfindung, die eine Gebührenkarte zum automatischen Ausgeben von postalischen Summen aufnimmt;

Fig. 5 ein Ablaufdiagramm des Betriebs der Station der Fig. 4;

Fig. 6a den Gebrauch von codierten Markierungen zur Beglaubigung von einer Postmarkierung, die von einer postalischen Transaktionsstation gedruckt wird, und

Fig. 6b eine exemplarische Form einer Beglaubigungscodierung;

Fig. 7 schematisch eine bevorzugte Ausführungsform einer automatisierten Begleitschein-Druckstation und einer optischen Waage, die erfindungsgemäß eine Mikroprozessorkarte und eine spezielle Dienstkarte benutzt;

Fig. 8 ein Ablaufdiagramm des Betriebes der Station von Fig. 7 ist;

Fig. 9 eine Standardform eines Begleitscheins und Zeigerindikatoren zum Ausfüllen seiner Informationsfelder;

Fig. 10 eine schematische bevorzugte Ausführungsform einer automatisierten Auffüllstation, die erfindungsgemäß eine Mikroprozessorkarte, eine Hauptkarte und eine Überwachungskarte benutzt;

Fig. 11 ein Ablaufdiagramm des Betriebs der Station in der Fig. 10; und

Fig. 12 das integrierte System von Mikroprozessorkarten, Speicherkarten und Stationen der Erfindung.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

In Übereinstimmung mit den grundsätzlichen Prinzipien der Erfindung verwendet ein automatisiertes Transaktionssystem eine Mikroprozessorkarte in einer automatisierten Transaktionsstation. Verschiedene Arten von Mikroprozessorkarten sind kommerziell verfügbar, und die Technologie zur Herstellung solcher Karten und deren Gebrauch in Stationeneinrichtungen ist gut verstanden. Zum Beispiel macht Micro Card Technologies Inc. in Dallas, Texas, die "Micro Card Mask M4"-Karte, was eine Standard-(ISO)-Größe ist, ähnlich zu einer Kreditkarte, die einen 8-Bit-Mikroprozessor, einen achtpoligen Pinausgang, ein 9600 bps asynchrones seriellcs Austauschprotokoll, 12,8 Kbit Nur-Lese-Speicher (ROM), 288 Bit Zufallszugriffsspeicher (RAM) und 8 Kbit löschbaren/programmierbaren ROM (EPROM) hat. Eine in einem Abschnitt der Karte bereitgestellte Anordnung elektrischer Kontakte schließt an die entsprechenden Kontakte in der Station an, zu erlauben, daß der Kartenmikroprozessor Daten mit der Station austauscht. Es versteht sich natürlich, daß andere Arten von Datenkommunikationsverbindungen benutzt werden können, wie beispielsweise mittels magnetischer Induktion.

Die in der vorliegenden Erfindung benutzte herkömmliche Mikroprozessorkarte funktioniert durch Ausführen eines intern gespeicherten Programms (firmware), auf das von außen nicht zugegriffen werden kann. Die "firmware" kann in beliebiger Form geschrieben werden, um sie gegen Manipulation von außen zu sichern. Ein elektrisch programmierbarer (EPROM) Speicherbereich, der mit dem Mikroprozessor der Karte in Verbindung gebracht wird, ist im allgemeinen in drei Zonen unterteilt: eine geheime Zone, auf die nur intern zugegriffen werden kann; eine geschützte Lese/Schreibzone, auf die nur zugegriffen werden kann nachdem eine Schlüsselzahl oder PIN bestätigt worden ist, und eine freie Lesezone. Die Karte wird in einer Station zum Ausführen gewünschter Funktionen benutzt, in Übereinstimmung mit den Regeln, Prozeduren und Daten, die in der Karte und der Station gespeichert sind oder von der Karte und der Station ausgeführt werden.

Wenn herkömmliche Mikroprozessorkarten an individuelle Benutzer ausgegeben werden, wird eine Gültigkeitsprozedur an einer

Berechtigungsstation ausgeführt. Die Prozedur benötigt im allgemeinen, daß der Erteiler die richtige Herstellungsseriennummer der Karte eingibt, zum Bestätigen, daß die Karte autorisiert ist. Eine PIN wird dann dem Kartenhalter zugeordnet oder von ihm ausgewählt, und in der geheimen Zone gespeichert. Des weiteren kann eine geheime Schlüsselzahl, die einzig der Erteiler kennt, die einer Gruppe oder einer chronologischen Folge von Kartenhaltern gemein sein kann, auch in der geheimen Zone gespeichert werden. In einigen Kartensystemen wird der geheime Schlüssel als ein Argument eines verschlüsselten Algorithmus benutzt, um ein verschlüsseltes Wort an die Station zum Bestätigen zu senden. Wenn das Wort zum Herleiten des geheimen Schlüssels durch die Station dekodiert werden kann, dann ist die Karte voraussichtlich echt. Nach der Vollendung der Gültigkeitsprozedur ändert die Karten-MPU irreversibel ihr Programm, so daß keine weiteren Wörter in die gemeime Speicherzone geschrieben werden können. Danach, nach Gebrauch der Karte, muß ein Benutzer die korrekte PIN eingeben, um zu bestätigen, daß die Karte von ihrem autorisierten Benutzer verwendet wird. Herkömmliche Mikroprozessorkarten haben auch das Kennzeichne, daß die Karte zum Gebrauch vorübergehend oder permanent gesperrt wird, falls eine Folge von nicht korrekten PIN-Eingaben an der Station erfaßt wird.

Zum Zeitpunkt der Ausstellung wird eine Summe in Geld oder anderen Einheiten für die auszugebende Karte bestätigt. In herkömmlichen Karten ist die Summe permanent in einen der mehreren Transaktionsbereichen in der geschützten Speicherzone geschrieben. Jedesmal wenn die Karte mit einer neuen Summe "aufgefüllt" werden soll, wird einer der Bereiche entriegelt und mit einer neuen Summe durch den Erteiler beschrieben. Somit kann jedesmal eine limitierte autorisierte Summe geschrieben werden, und die Karte wird dann mehrere Male aufgefüllt, bevor ihre Speicherkapazität aufgebraucht ist. Dies ist ein Sicherheitskennzeichen zum Minimieren von Geldverlust, für den Fall, daß die Karte verloren geht oder gestohlen wird. Die autorisierte Summe wird bei jeder Transaktion vermindert, und ein neues Guthaben wird notiert, bis das Guthaben aufgebraucht ist. Obwohl jede Summe oder Guthaben in den Transaktionsspeicher der Karte geschrieben werden kann, kann die Karte, kann als weiteres Sicherheitskennzeichen, die Karte verhindern, daß ein Guthaben notiert wird, das eine vorgegebene Grenze oder ein zuvor notiertes Guthaben übersteigt.

Ein kartenautomatisiertes Transaktionssystem, das die besonderen Kennzeichen der Erfindung vereint, soll nun beschrieben werden. Es ist zu verstehen, daß die Erfindung, obwohl besondere Ausführungsformen

beschrieben werden, nicht auf solche Ausführungsformen limitiert ist, sondern alle Modifikationen und Variationen beinhaltet, die die Prinzipien der Erfindung benutzen. Zum Zwecke dieser Beschreibung wird die Transaktionsstation als Portozumeßstation gewählt, zum Drucken einer Portomarkierung auf ein Etikett, einen Umschlag oder einen Begleitschein für zu verschickende oder zu verschiffende Artikel. Jedoch ist zu verstehen, daß die allgemeinen Prinzipien der Erfindung breite Anwendung für irgendwelche Arten von Transaktionsstationen haben, in denen eine Mikroprozessorkarte benutzt werden kann. Zum Beispiel kann die Station auch eine Bargeld- oder Gegenstandsausgabemaschine oder ein Drucker sein, der Berechtigungsmarkierungen, Coupons, Belege, Eintrittskarten, Bestandsverzeichnisse, ect. druckt.

Portozumeßstation

Bezugnehmend auf Fig. 1 ist eine Mikroprozessorkarte 10 angepaßt, wie zuvor beschrieben, um in einen Karteneinführungsschlitz 11 einer automatisierten Stationeneinrichtung 20 eingeführt zu werden. Die Smart-Karte 10 hat einen Kontaktabschnitt 12, der eine Anzahl von Kontakten 13 hat, die mit den PIN-Ausgangsleitungen eines IC-Bauelements verbunden sind, das eine Mikroprozessoreinheit (Karten-MPU) 60 umfaßt, die unter einer Schutzschicht des Karten-Kontaktbereichs 12 laminiert ist. Die Kontakte 13 werden mit den entsprechenden Kontakten 23 eines Stationen-Kontaktbereichs 22 vereint, nach Einführen der Karte 10 in Pfeilrichtung A in den Schlitz 11. Sowie die Karte eingeführt wird, stößt ihre Vorderkante an einen Teil der Station-Kontaktbereichs 22, der in die gleiche Richtung bewegt wird, was durch den Pfeil B angezeigt ist, um somit in einen betriebsfähigen elektrischen Kontakt mit dem Karten-Kontaktbereich 12 in Verbindung zu treten. Ein Auslöseschalter 22a ist an dem Boden des Schlitzes 11 bereitgestellt und löst ein Startsignal für einen Betriebs-Mikroprozessor (Stations-MPU) 30 aus, wenn die Karte ganz in Position in den Schlitz eingeführt worden ist.

Die Karten-MPU 60 führt ein intern gespeichertes Programm (firmware) aus, um zu prüfen, ob eine verlangte Transaktion autorisiert ist, und um eine sichere Handshake-Erkennungsprozedur (die weiter unten beschrieben wird) mit einem Mikroprozessor in der Station durchzuführen, vor dem Belasten des Kartenkontoguthabens. Obwohl die Handshake-Prozedur mit einem Betriebs-Mikroprozessor für die Station oder für eine von der Station entlegene gelegene, durchgeführt werden kann, wird es in der Erfindung bevorzugt, daß die Prozedur mit einem sicheren in dem gegenwärtigen

Wertausgabeabschnitt der Station eingebetteten Mikroprozessor durchgeführt wird. Der Wertausgabeabschnitt ist ein getrenntes Element in der Station, und sein Mikroprozessor ist körperlich gesichert, wie beispielsweise durch Einbetten in Epoxyharz, so daß jeder Versuch ihn zu manipulieren darin resultieren würde, daß sich der Wertausgabeabschnitt als betriebsunfähig erweist. Für die postalische Transaktionsstation der Erfindung ist der Mikroprozessor in die Druckereinheit eingebettet, die die Postmarkierung druckt.

Die Stationenkontakte 23 sind mit den Funktionsteilen der Station verbunden, die eine taktisynchronisierte Verbindung 24, eine Rücksetzverbindung 25, eine Betriebsspannungsverbindung V_{CC} 26, einen Eingabe/Ausgabe (I/O) Anschluß 27, eine EPROM-Schreibspannungsverbindung V_{pp} 28 und eine Erdungsverbindung 29 umfaßt. Die Stations-MPU 30 steuert die Schnittstelle mit der Karte und den Betrieb der verschiedenen Teile der Station, einschließlich einer Tastatur 31, einer Anzeige 32, wie beispielsweise eine LCD, und einem Portostempeldrucker 40, der der Wertausgabeabschnitt der Station ist. Eine Spannungsquelle V_0 wird durch eine Batterie und/oder eine externe AC oder DC Leitung bereitgestellt, um die verschiedenen Teile der Station zu betreiben.

Der Drucker 40 hat eine Mikroprozessoreinheit (Drucker MPU) 41, die individuell und alleinig den Betrieb des Druckkopfs 42, beispielsweise einen elektrothermischen oder Auftreffdruckkopf, steuert. Die MPU 41 führt wie der Kartenmikroprozessor ein internes Programm (firmware) aus, so daß sie nicht von außen manipuliert werden kann. Das interne Programm der Drucker MPU umfaßt einzigartige Verschlüsselungsalgorithmen, die denen im Mikroprozessor der Karte gespeicherten entsprechen, das von dem Hersteller installiert wird, so daß die Drucker MPU eine sichere Handshake-Erkennungsprozedur mit dem Mikroprozessor der Karte ausführen kann, um eine verlangte Transaktion zu autorisieren. Die MPU 41 ist auch als einheitliches Ganzes mit dem Druckkopf 42 ausgebildet, beispielsweise durch Einbetten in Epoxyharz oder dergleichen, so daß auf sie nicht körperlich zugegriffen werden kann, ohne den Druckkopf zu zerstören. Somit kann erfindungsgemäß der Druckkopf 42 der Portozumeßstation 20 nur durch die MPU 41 betrieben werden, und ein Portostempel wird nur gedruckt, wenn die Handshake-Erkennungsprozedur und ein Portostempel-Druckbefehl zwischen der Karten MPU und der Drucker MPU 41 ausgeführt worden sind.

Wenn eine Station durch einen Erteiler an einem Ort installiert werden soll, oder an einen Einzelhandelszwischenhändler zum Weitergebrauch

ausgeteilt werden soll, kann der Erteiler auch eine Gültigkeitsprozedur für die Station ausführen, die der für die Karte ähnlich ist. Eine geheime Schlüsselzahl kann in die geheime Speicherzone der Drucker MPU 41 geschrieben werden, so daß Portodrucktransaktionen nur mit Karten ausgeführt werden können, die mit der entsprechenden geheimen Schlüsselzahl ausgestattet sind. Somit werden Karten, die von anderen Erteilern für gültig erklärt worden sind, auch wenn sie vom gleichen Hersteller erhalten wurden, nicht in den zuerst genannten Maschinen des Erteilers benutzbar sein.

Die Stations MPU kann natürlich für die Handshake-Erkennungsprozedur verwendet werden. Jedoch wird bevorzugt, die Prozedur von dem Teil ausführen zu lassen, der tatsächlich den Wertgegenstand ausgibt, und die Stations MPU funktionsfähig zu lassen für allgemeine Stationenbetriebe. Eine Maschinen ID-Nummer (MIN) kann auch der Station zugewiesen sein, so daß sie in der Karte aufrechterhaltenden Transaktionsvergangenheit aufgezeichnet werden kann. Als ein weiteres Kennzeichen kann die MIN für eine oder mehrere der Stationen des Erteilers in der Karte gespeichert werden, die nur in solchen Stationen benutzt werden sollen. Somit können in einem an eine Firma ausgegebenes automatisiertes Stationensystem die Stationen innerhalb der Firma nur mit den Karten benutzt werden, die an die Angestellten dieser Firma erteilt wurden, die die geheime Schlüsselnummer der Firma haben, und wahlweise können die Stationen innerhalb einer Firmenabteilung konfiguriert werden, um nur Karten zu akzeptieren, die mit den MINS der Maschinen dieser Abteilung ausgestattet sind.

Der interaktive Betrieb des Karten/Stationensystems soll nun beschrieben werden. Nach dem Einführen einer Karte in Schlitz 11 wird der Auslöseschalter 22a ausgelöst und die Stations MPU 30 initiiert eine Identifikationsbedarfsprozedur zum Bestätigen, daß die Karte von einem autorisierten Benutzer benutzt wird. Zum Beispiel kann die Stations MPU veranlassen, daß eine Aufforderung auf der Anzeige 32 erscheint, die verlangt, daß der Benutzer eine PIN eingibt. Die durch den Benutzer eingegebene Zahl wird von der Stations MPU an die Karten MPU gesendet, wo sie mit der in der geheimen Zone des Kartenspeichers gespeicherten PIN-Zahl(Zahlen) verglichen wird. Wenn die Zahl übereinstimmt teilt die Karten MPU der Stations MPU 30 mit fortzufahren. Wenn die Karte nur zum Gebrauch von bestimmten Maschinen begrenzt ist, könnte die Station die PIN oder eine Kartenidentifikations- oder Kontonummer mit einer Liste gespeicherter Kartennummern vergleichen. Als ein weiteres Sicherheitskennzeichen könnte

das Kartenprogramm die Anzahl von inkorrekten PIN-Eingabeversuchen, oder ein zum Ausstellungszeitpunkt in den Speicher geschriebenes Kartenablaufdatum, kontrollieren. Wenn die inkorrekten PIN-Eingaben eine vorgegebene Zahl überschreiten, oder wenn das von der Stations MPU angezeigte gegenwärtige Datum älter als das Ablaufdatum ist, kann die Karten MPU 60 die Karte gegen weiteren Gebrauch sperren, bis der Benutzer sie durch einen Erteiler für wiedergültig erteilen läßt.

Wenn die anfänglichen Bestätigungsprozeduren verstrichen sind, fordert die Stations MPU 30 als nächstes den Benutzer auf, Informationen für eine Portotransaktion einzugeben. Der Benutzer gibt am Eingabefeld 31 die Summe des verlangten Portos ein, und als weitere Möglichkeit die Postleitzahl des Orts des Absenders und das Datum. Sowie die Information aufeinanderfolgend bereitgestellt wird, d.h. "Summe", "Postleitzahl" und "Datum", wird sie zur Bestätigung an der Anzeige 32 angezeigt. Alternativ kann das Datum von der Stations MPU 30 erhalten werden und zur Benutzerbestätigung angezeigt werden. Wenn all die richtigen Informationen eingegeben worden sind wird ein Rand eines zu versendenden Umschlags 51, der ein Etikett, oder ein Postformular, das dem zu versendenden Artikel beigefügt werden soll, in einen Schlitz 50 auf einer Seite der Postzumeßstation 20 eingeführt. Die Bewegung des Etiketts oder des Umschlags kann gesteuert werden, um ihn in Registrierung mit dem Druckkopf zu bringen, wie das in herkömmlichen Zumeßmaschinen bereitgestellt ist. Der Benutzer drückt dann die "Druck"-Taste, um eine Portodrucktransaktion zu initiieren.

Handshake-Erkennungsprozedur

Ein grundlegendes Prinzip der Erfindung ist, daß die gegenwärtige Durchführung einer Wert-Austauschtransaktion durch eine gegenseitige Handshake-Erkennungsprozedur zwischen einem sicheren Mikroprozessor, der das Kontoguthaben der Karte unterhält, und einem sicheren Mikroprozessor, der den Wertausgabebetrieb steuert, sicher gesteuert wird. Die Karten MPU muß den Mikroprozessor des Wertausgabeabschnitts für gültig erkennen, und umgekehrt, um eine Transaktion auszuführen. Deswegen können die Karte und der wertausgebende Abschnitt beide autonom und geschützt bleiben gegen Fälschen oder betrügerischen Gebrauch, auch dann, wenn die Sicherheit des anderen durchbrochen worden ist. Da sie autonom sind können die Karten und Stationen mit einem geringen Risiko des Durchbrechens des Systems und ohne Notwendigkeit einer strikten Zugangskontrolle weit verbreitet werden. Somit hat es signifikante Kosten und Sicherheitsvorteile gegenüber herkömmlichen Karten-Transaktionssystemen.

Eine Ausführungsform für einen zweiwegig verschlüsselten Handshake soll nun beschrieben werden. Es soll jedoch verstanden werden, daß die Erfindung beabsichtigt, jegliche gegenseitige Handshake-Prozedur einzuschließen, durch die die Karten- und Ausgabemikroprozessoren den anderen als autorisiert erkennen, um eine verlangte Transaktion auszuführen. In der bevorzugten Ausführungsform einer Portostation wird die Handshake-Prozedur zwischen der Karten MPU 60 und der Drucker MPU 41 ausgeführt. Wenn das "Druck"-Schlüsselssignal von der Stationen MPU 30 empfangen wird, öffnet die letztere einen Kommunikationskanal 61 zwischen der Karten MPU 60 und der Drucker MPU 41, wie in Fig. 2a schematisch dargestellt. Ein "Beginn"-Signal und die Summe der verlangten Transaktion, d.h. Porto, wird dann von der Stationen MPU 30 zu der Karten MPU 60 gesendet, und ein ähnliches "Beginn"-Signal wird an die Drucker MPU 41 gesendet, um den Gang auf eine Handshake-Prozedur vorzubereiten.

Bezugnehmend auf Fig. 2b initiiert die Karten MPU 60 die Handshake-Prozedur nach Empfang des "Beginn"-Signals, in dem zuerst verifiziert wird, ob die verlangte Summe für die Transaktion verfügbar ist. Als ein vorteilhaftes Kennzeichen der Erfindung prüft die Karten MPU 60 das verfügbare Guthaben der Karte, und (wenn es in dem Programm der Karte implementiert ist), ob die verlangte Transaktion innerhalb etwaiger durch den Kartenerteiler spezifizizierte Grenzen liegt. Zum Beispiel kann der Gebrauch der Karte auf eine maximale Portosumme und/oder Portokategorie für jede Transaktion oder eine angesammelte Summe von Transaktionen limitiert werden. Nach Verifizieren, daß die verlangte Transaktion autorisiert ist, verschlüsselt die Karten MPU 60 eine Gegenstandszahl N, die eine Zufallszahl sein kann, mit einer Schlüsselzahl k1 (die die Benutzer PIN sein kann), die in der geheimen Zone ihres Speichers durch einen ersten Verschlüsselungsalgorithmus E1 gespeichert ist, und sendet das resultierende Wort W1 über den Handshake-Kanal 61 der Stationen MPU 30 an die Drucker MPU 41.

Nach dem Empfang des Wortes W1 dekodiert die Drucker MPU 41 die Zahl, unter Verwendung der gleichen Zahl k1, mittels dem inversen Algorithmus E1'. Die Zahl k1 kann eine geheime Schlüsselzahl sein, die zum Zeitpunkt der Gültigkeitserklärung in dem Speicher der Drucker MPU oder in einem offenen System gespeichert wurde, sie kann die von einem Benutzer an der Station eingegebene PIN sein, oder eine Kombination von beiden. Dann verschlüsselt die Drucker MPU 40 die dekodierte Zahl mit der Zahl k1

mittels eines zweiten Verschlüsselungsalgorithmus E2, um ein zweites Wort W2 zurück an die Karten MPU 60 zu senden.

Nach dem Empfang des Worts W2 dekodiert die Karten MPU 60 die Nummer wieder, unter Verwendung der Schlüsselzahl k1 mittels des inversen zweiten Algorithmus E2', und vergleicht die dekodierte Zahl mit der Zahl, die sie in der ersten Übermittlung verwendet hat. Wenn die Zahlen übereinstimmen ist die Handshake-Prozedur erfolgreich abgeschlossen worden und die Karten- und Drucker MPUs haben sich gegenseitig als autorisiert erkannt, zum Ausführen der verlangten Transaktion. Die Karten MPU belastet dann das Kartenguthaben mit der Portosumme und sendet dann einen Druckbefehl und die Portosumme an die Drucker MPU. Die Drucker MPU druckt das Porto auf einen Umschlag 51 in Zusammenarbeit mit der Stationen MPU 30, die die Bewegung des Umschlags unter dem Druckkopf steuert. Dann sendet die Drucker MPU ein "End"-Signal an die Stationen MPU 30, die dementsprechend den Handshake-Kanal 61 ausschaltet, und führt sich selber zum Empfang der nächsten Transaktionsnachfrage in den Ausgangspunkt zurück.

In der bevorzugten Ausführungsform speichert die Karten MPU 60 nur die Summe der Transaktion in ihrer Transaktionsaufzeichnung, und nicht das neue Guthaben. Stattdessen wird das Guthaben zum Zeitpunkt, zu dem die Transaktion verlangt wird, von der ursprünglich autorisierten Summe und der gespeicherten Vorgeschichte von Transaktionslasten neu berechnet. Diese Prozedur ersetzt die Rechenleistung der MPU, um eine signifikante Menge des Speicherplatzes des Karten EPROMs zu sparen.

Das erfindungsgemäße automatisierte Transaktionssystem ist mit hoher Sicherheit unterschiedlicher Stufen ausgestattet, was insbesondere für Off-Line-Transaktionen vorteilhaft ist, die eine große Anzahl von erteilten Karten und weitverbreitete Stationeneinrichtungen beteiligen. Wie in Fig. 3 dargestellt sind die Verschlüsselungsalgorithmen einer ersten Sicherheitsstufe I von dem Hersteller bereitgestellt, der geheime Schlüssel, PIN und/oder MIN wird bei Sicherheitsstufe II von dem Erteiler bereitgestellt, die PIN wird bei Sicherheitsstufe III von einem einzelnen Benutzer benutzt, und die MIN und/oder ein geheimer Schlüssel können bei Sicherheitsstufe IV benutzt werden, um (eine) besondere Maschine(n) zu betreiben.

Bei Stufe I ist der Druckkopf der Station nur betreibbar zum Ausgeben von Werten, d.h. Druckportos, wenn der von dem Hersteller bereitgestellte Verschlüsselungsalgorithmus mit denen der Karte übereinstimmt, wodurch vor Fälschen von Karten und Stationen geschützt wird. Sogar wenn die Sicherheit

des Herstellers durchdrungen worden ist, und die Verschlüsselungsalgorithmen von einem Betrüger erlangt worden sind, kann der geheime Schlüssel bei Stufe II durch den Erteiler zugeteilt werden und in der Handshake-Prozedur verwendet werden, wodurch der Gebrauch von gefälschten Karten und Stationen, die den geheimen Schlüssel nicht haben, abgeschreckt wird. Bei Sicherheitsstufe III kann eine Karte nur benutzt werden, um eine Station zu betreiben, falls die richtige PIN bekannt ist, und falls die anfänglichen Bestätigungsprozeduren verstrichen sind. Bei Sicherheitsstufe IV kann eine Karte nur in einer bestimmten Station benutzt werden, die durch die richtige MIN identifiziert wird.

Eine ähnliche Ausführungsform gemäß der Erfindung ist in Fig. 4 dargestellt, die eine zweite Karte mit postalischen Gebührendaten verwendet, die im Speicher gespeichert sind, um das richtige Porto automatisch zu berechnen. Eine Station 20, die ähnlich der zuvor beschriebenen ist, umfaßt einen zweiten Schlitz 91 für eine "Gebühren"-Karte 90. Die Station hat einen Schlitz 50, in den ein postalisches Etikett oder Umschlag 51 eingeführt wird, zum Aufdrucken durch den Drucker 40. Für ein Paket 52 wird das Etikett 51 gedruckt und dann an dem Paket zum Versenden angebracht. Eine Waage 53 kann mit der Station und der MPU 30 verbunden sein, um das Gewicht des Umschlags oder Pakets 52 bereitzustellen.

Die Gebührenkarte hat eine Speichereinrichtung 92, vorzugsweise ein IC ROM, auf das zugegriffen wird und das von der Stationen MPU 30 über Kontaktabschnitte 93, die mit den PIN Ausgabestationen der Speichereinrichtung kontaktierend verbunden sind, gelesen wird. Schalter 22a und 92a liefern Signale wenn die Benutzer- und Gebührenkarten in die entsprechenden Schlitze eingeführt worden sind. Ein Einführen der Benutzerkarte löst den Betrieb der Station aus. Wenn eine Gebührenkarte nicht eingeführt ist, kann die Stationen MPU 30 stattdessen die angemessene Postsumme von dem Benutzer verlangen, durch eine Aufforderung an der Anzeige 32. Die Stationen MPU kann auch einen Modus zum Lesen von Portogebühren von der Gebührenkarte haben.

Der Programmbetrieb der Portozumeßstation 20 ist in Blockdiagrammform in Fig. 5 dargestellt. Nach Einführen der Benutzerkarte 10 in Schlitz 11 werden die zuvor beschriebenen Benutzerbestätigungs-Prozeduren zwischen der Stationen MPU 30 und der Karten MPU 60 ausgeführt. Wenn eine nicht autorisierte(r) Karte oder Benutzer erfaßt wird, wird die Karte gesperrt und der Betrieb der Station wird beendet. Wenn eine gültige Benutzerkarte

bestätigt wird, dann prüft das Stationenprogramm, ob eine Gebührenkarte 90 eingeführt ist und ob sie gültig ist. Gültigkeit kann durch die Erteilungsnummer der Karte oder durch ein angezeigtes Ablaufdatum festgestellt werden. Wenn keine Karte da ist fordert die Stationen MPU den Benutzer auf das gewünschte Porto einzugeben, und geht zu dem Drucktasten-Entscheidungsblock 97. Wenn eine gültige Gebührenkarte anwesend ist, verlangt das Stationenprogramm die Codes für den Ursprung und Bestimmung des Artikels und die gewünschte Postkategorie. Dann prüft das Programm nach einem Signal von der Waage 53, die das Gewicht des Artikels anzeigt. Wenn keine Waage angeschlossen ist, oder kein Gewicht angezeigt wird, fordert das Programm den Benutzer auf die Information einzugeben.

Der Speicher der Gebührenkarte umfaßt eine aktuelle Gebührenliste für einen einzelnen Überbringer, die gemäß Zonenklassifikationen, Gewicht und/oder Postart unterteilt ist. Für den U.S. Postdienst wird die Portosumme basierend auf den Ursprungs- und Bestimmungspostleitzahlen, Postkategorie und Gewicht berechnet, durch Nachschlagen von Tabellen, die in dem Speicher 92 der Gebührenkarte gespeichert sind. Wenn die "Drucktaste" gedrückt wird, dann sendet das Stationenprogramm das "Beginn"-Signal an die Karten MPU und Drucker MPU, um die Handshake-Prozedur und Belast- und Druckbetrieb auszuführen, wie zuvor beschrieben. Wenn eine "Automatisch"-Betriebs-Taste der Station gedrückt worden ist oder der Benutzer auswählt fortzufahren, in Reaktion zu einer Aufforderung, kehrt das Stationenprogramm zum Anfang der bei Block 94 angezeigten Transaktionsschleife zurück. Der "Automatik"-Modus kann im Zusammenhang mit einem automatischen Zuführer verwendet werden, zum Portostempeln einer Reihe von Umschlägen oder Etiketten. Der Stationenbetrieb wird beendet, wenn die Transaktionsschleife nicht fortgeführt wird, oder wenn die Handshake-Prozedur nicht abgeschlossen ist.

Portostempelechteit

In Übereinstimmung mit den auf Portozumeßstationen angewendeten Prinzipien der Erfindung wird nun eine Portostempel-Echtheitsprozedur beschrieben. Die Prozedur wird als Sicherheitskennzeichen bereitgestellt, um das Drucken von gefälschten Portostempeln durch einen Drucker, Kopierer, oder anderen Facsimile-Einrichtungen abzuschrecken, das nicht durch den Erteiler des zuvor beschriebenen Karten/Stationensystems autorisiert wird. Herkömmliche hochauflösende Drucker und graphische Fähigkeiten von Personal-Rechnern stellen ein zunehmendes Risiko dar, daß wertbestätigende Markierungen, wie beispielsweise ein Portostempel, Karten, Coupons, etc.

durch einen Fälscher simuliert werden können. In der Erfindung wird ein unterliegender und/oder unsichtbarer maschinenlesbarer Code zuerst gedruckt und dann mit einem von einem Menschen lesbaren Portostempel überdruckt. Der Code kann einzig durch den Erteiler des Porto-Karten/Stationensystems ausgewählt werden und periodisch geändert werden, um jeglichen Vorteil vom Gewinn nicht autorisierten Zugriffs auf den Code zu eliminieren. Des weiteren kann der Code mit Tinte gedruckt werden, die unsichtbar im normalen Lichtspektrum ist, so daß er nur lesbar ist mit einem magnetischen, Infrarot- oder ultravioletten Leser.

Bezugnehmend auf ein in Fig. 6a und 6b gezeigtes Beispiel hat ein herkömmlich aufgedruckter Portostempel ein Logo oder ein graphisches Design 70, einen Text 71, der anzeigt, daß das Porto von dem U.S. Postdienst erteilt wurde, Nummern 72, die die Portosumme anzeigen, sowie das Datum 73, Stadt 74, Staat 75 und Postleitzahl 76 des Ursprungs, und die Identifikationsnummer 77 der Frankiermaschine, von der der Portostempel gedruckt wurde. In der Erfindung werden codierte Markierungen 78 unter dem sichtbaren Portostempel in einem vorbestimmten Code-Feld 79 in unsichtbarer, maschinenlesbarer Tinte gedruckt. Der Algorithmus für die codierten Markierungen wird z.B. von dem Erteiler ausgewählt, die das binäre Äquivalent der Portosumme darstellen, d.h. "90" Cents in Fig. 6a, was in binärer Form in Fig. 6b gezeigt ist. Die codierten Markierungen können irgendein anderes Element des Portostempels darstellen, wie beispielsweise die Maschinenidentifikationsnummer oder Postleitzahl. Alternativ kann ein Strichcode 83 mit einem Portostempel- Informationsabschnitt 83a und einem Prüf-Code-Abschnitt 83b gedruckt werden, der verschlüsselt ist, basierend auf einem der Portostempelelemente. Das Portostempelelement und/oder der Verschlüsselungsalgorithmus kann einzig von dem Erteiler ausgewählt werden. Sogar wenn die codierten Markierungen in sichtbarer Weise gedruckt sind, wird die Verschlüsselung von einem variierbaren Portostempelelement, wie beispielsweise der Postleitzahl des Absenders, Datum, oder Portosumme, ein Kopieren schwer machen.

Das Drucken des Portostempels und Echtheitscodes kann bereits in dem in Fig. 1 dargestellten Karten/Stationensystem enthalten sein. Der Drucker 42 ist mit einem Speicher 43 ausgestattet, an den Daten, die die sichtbare Information des Portostempels und den berechneten binären oder anders ausgewählte Testcodes oder umgewandelte Strichcodes darstellen, von der Stationen MPU 30 übermittelt werden und gespeichert werden. Die festen

Graphiken des Portostempels können in einem Speicher gespeichert werden, der mit der MPU 30 assoziiert wird, was vorzuziehen ist, wenn die gleiche Station die Fähigkeit hat verschiedene Portostempelgraphiken für verschiedene Überbringer und/oder Dienstkategorien zu drucken, oder sie kann permanent in einem Abschnitt des Druckerspeichers 43 gespeichert werden. Stattdessen können die festen Graphiken für eine verlangte Transaktion in dem Kartenspeicher gespeichert werden und von der Stationen MPU 30 in den Druckerspeicher 43 geladen werden. Alternativ können die festen Graphiken auf einer Platte bereitgestellt werden, die mit dem Druckkopf arbeitet, wenn nur ein Portostempeltyp gedruckt werden soll.

In der bevorzugten Form ist der Druckkopf 42 ein Auftreffdrucker, der zwei Farbbänder 42a und 42b hat, eines aus unsichtbarer, maschinenlesbarer Tinte und das andere aus sichtbarer Tinte. Wenn die Handshake-Prozedur abgeschlossen worden ist und der Druckbefehl durch die Karten MPU 60 erteilt wurde, greift die Drucker MPU 41 auf die in dem Speicher 43 gespeicherten Daten zu, und druckt die codierten Markierungen in einem ersten Durchgang mit unsichtbarer Tinte, und druckt dann in einem zweiten Durchgang die sichtbare Portostempelinformation..

Wenn Post oder andere Gegenstände anschließend einer zentralen Postroutine und einem Verteilungssystem präsentiert werden, wie beispielsweise dem des U.S. Postdienstes oder einem privaten Überbringer, kann der Portostempel, wie in Fig. 6a angedeutet, unter einem Detektor 80 vorbeigeführt werden, der einen Leser 81 im sichtbaren Lichtspektrum hat und einen Codierleser 82, beispielsweise einen magnetischen, Infrarot- oder Ultraviolett-Leser, oder einen Strichcodeleser 83 für Strichcodemarkierungen. Wenn die Codiermarkierungen fehlen, oder wenn der Prüfcode nicht dem zum Codieren ausgewählten Element des Portostempels entspricht, kann eine Prüfaufzeichnung der Nichtübereinstimmung gemacht werden, z.B. durch Aufzeichnen der Maschinenidentifikationsnummer, Datum und Postleitzahl des Ursprungs. Eine Untersuchung der Quelle des nicht autorisierten Portos kann dann initiiert werden, wenn festgestellt wird, daß zahlreiche Gegenstände nicht autorisierte Portostempel tragen. Die Portostempel-Beglaubigungsmarkierungen der Erfindung stellen somit eine zusätzliche Sicherheitsstufe gegen Fälschen bereit, die nicht in herkömmliche Portozumeßmaschinen geboten wird.

Portobegleitschein-Station

Eine weitere Ausführungsform der Erfindung ist in Fig. 7 dargestellt, die angepaßt ist, Standardbegleitscheinformulare für Postgegenstände zu

drucken, unter der Benutzung einer großen Anzahl von postalischen oder privater Überbringerdiensten. Eine Station 20' umfaßt einen Schlitz 11 für eine Benutzerkarte 10, eine Stationen MPU 30, einen Drucker 40 und eine Drucker MPU 41, eine Tastatur 31' und eine Anzeige 32', wie zuvor im Zusammenhang mit Fig. 1 beschrieben. Die Station umfaßt auch einen zweiten Schlitz 91 für eine "Gebühren"-Karte 90 und einen dritten Schlitz 101 für eine "Sonderdienst"-Karte 100. Die Station hat einen Schlitz 50, in den ein Standardbegleitscheinformular 51' eingeführt wird zum Bedrucken durch den Drucker 40. Der Begleitschein 51' wird dann zum Versenden an einen Umschlag oder ein Paket 52 angebracht. Eine Waage 53 kann an die Station und die MPU 30 angeschlossen werden, um automatisch das Gewicht des Pakets 52 bereitzustellen.

Die Gebühren- und Sonderdienstkarten haben Speichereinrichtungen 92 bzw. 102, die vorzugsweise IC ROMs sind, auf die zugegriffen wird und die von der Stationen MPU 30 über Kontaktabschnitte 92 bzw. 103, die in Kontaktverbindung mit den Pinausgangsstationen der Speichereinrichtungen verbunden sind, gelesen werden. Schalter 22a, 92a und 102a stellen Erfassungssignale bereit, wenn die Karten in die entsprechenden Schlitz e eingeführt worden sind. Eine Anzeige 32' liefert einen vollen Bereich, der dem Aussehen des Begleitscheinformulars entspricht, und die Tastatur 31' umfaßt einen kompletten Satz alphanumerischer Zeichen und Befehlstasten.

Der Speicher der Gebührenkarte beinhaltet eine aktuelle Liste für die Gebühren eines speziellen Überbringers. Wenn z.B. der Überbringer der U.S. Postdienst ist, sind die Postamtsgebühren gemäß Zonenklassifikation, Gewicht und Postkategorie aufgelistet. Der Speicher der Sonderdienstkarte beinhaltet ein Programm zum Ausfüllen eines Standardbegleitscheinformulars in Übereinstimmung mit der durch den Postdienst eines bestimmten Überbringers benötigten Information und mit Zeichen, die den Postdienst eines bestimmten Überbringers identifizieren. Wenn der Überbringer beispielsweise der U.S. Postdienst ist kann die Sonderdienstkarte die Programme zum Drucken von Begleitscheinen für Exprespost, beglaubigter Post, eingetragener Post, versicherter Post, etc. bereitstellen.

Der Programmbetrieb der postalischen Begleitscheinstation 20' ist in Blockdiagrammform in Fig. 8 dargestellt, und ein Beispiel eines Begleitscheinformulars ist in Fig. 9 gezeigt. Nach Einführen der Benutzerkarte 10 in Schlitz 11 werden die zuvor beschriebenen Benutzerbestätigungsprozeduren zwischen der Stationen MPU 30 und der Karten MPU 60 ausgeführt. Wenn eine nicht autorisierte Karte oder Benutzer erfaßt

wird, wird die Karte gesperrt und der Stationenbetrieb werden beendet. Mit einer gültigen Benutzerkarte prüft dann das Stationenprogramm, ob eine Gebührenkarte 90 und/oder eine Sonderdienstkarte 100 eingeführt ist, und ob jede gültig ist. Gültigkeit kann durch die Erteilernummer oder durch ein angezeigtes Ablaufdatum festgestellt werden. Wenn keine Gebührenkarte oder Sonderdienstkarte vorhanden ist, fordert die Stationen MPU den Benutzer auf das gewünschte Porto einzugeben und geht zu dem Drucktastenentscheidungsblock 121 über. Die Station wird dann zum Drucken eines Portostempels oder eines Portoetiketts benutzt, wie zuvor beschrieben. Wenn eine gültige Dienstkarte gegenwärtig ist, zeigt das Stationenprogramm ein Post- oder Überbringerdienst-Menü von der Dienstkarte an und fordert den Benutzer auf, einen Dienst auszuwählen.

Die Stationen MPU 30 lädt das ausgewählte Dienstprogramm von der Dienstkarte und führt es aus, wie bei Block 118 angezeigt. Für typische Überbringerdienste zeigt das Dienstprogramm ein Standardüberbringer-Begleitscheinformular an, das von dem ausgewählten Überbringer benutzt wird. Wenn beispielsweise der U.S. Postdienst-Expresspostdienst ausgewählt wird, wird das in Fig. 9 gezeigte Formular angezeigt. Das Formular umfaßt ein Überbringeridentifikationsfeld 130, ein Dienstkategoriefeld 131, und Zeiger an der Anzeige zum Einfügen von Information in Felder 132 bis 137 und 140 bis 146. Eine Begleitschein-Identifikationsnummer in Form von Strichcode 138 und Zeichen 139 wird für die Transaktion ausgewählt und angezeigt. Vorzugsweise hat die Dienstkarte eine Liste von reservierten Begleitscheinnummern, die aufeinanderfolgend für jede abgeschlossene Transaktion erhöht werden. Wenn eine Transaktion nicht abgeschlossen wird, wird die Nummer für die nächste Transaktion gespeichert. Wie zuvor beschrieben, kann der Strichcode einen Abschnitt enthalten, der eine Verschlüsselung eines Elements der Begleitscheininformation ist, so daß die Echtheit des Formulars durch eine Maschinenbearbeitung des Begleitscheins nachgeprüft werden kann.

Das durch die Stationen MPU 30 ausgeführte Dienstprogramm benutzt als nächstes Zeigeraufforderungen, um den Benutzer aufzufordern Information für bestimmte Felder bereitzustellen, wie beispielsweise die Postleitzahlen des Ursprungs- und Bestimmungsorts 123 und 133, und die Adressen des Absenders und Empfängers 140 und 141. Sowie der Benutzer jeden Punkt an Information liefert und eine "Eingabe"-Taste drückt, veranlaßt das Programm, daß der Zeiger zum nächsten zu liefernden Informationsfeld verschoben wird, wie durch Pfeil C in Fig. 9 dargestellt. Die Datums- und Zeitfelder 134 und 135

können vom Benutzer verlangt werden, oder können von der Station bereitgestellt werden, wenn sie mit einer Uhr und einem Kalender ausgestattet ist. Das Gewicht 136 kann vom Ausgang der Waage 53 geliefert werden, wenn mit der Station verbunden, oder durch den Benutzer geliefert werden. Die Maschinenidentifikationsnummer (MIN) wird von der Station für Feld 137 geliefert.

Basierend auf den Ursprungs- und Bestimmungspostleitzahlen und dem Gewicht werden die Portosumme, andere Dienstkosten und die Gesamtsumme 144 bis 146 berechnet und angezeigt unter Programmsteuerung, unter Benutzung der Gebührenkarte, falls angemessen. Die Gesamttransaktionssumme wird gespeichert. Wenn die "Druck"-Taste gedrückt wird sendet das Stationenprogramm das "Beginn"-Signal an die Karten MPU 50 und die Drucker MPU 41, um die Handshake-Prozedur und Belast- und Druckbetrieb auszuführen, wie zuvor beschrieben. Wenn eine "Automatik"-Betrieb-Taste der Station niedergedrückt wird, oder der Benutzer in Reaktion auf eine Aufforderung auswählt fortzufahren, kehrt das Stationenprogramm an den Anfang der bei Block 113 angezeigten Transaktionsschleife zurück. Der Stationenbetrieb wird abgeschlossen wenn die Transaktionsschleife nicht fortgeführt wird, oder wenn die Handshake-Prozedur nicht abgeschlossen ist.

Die Station kann zum Programmieren und Drucken der Begleitscheine von anderen gewählten Überbringen oder Diensten benutzt werden, durch Einführen der richtigen Benutzer-, Gebühren- und/oder Dienstkarten. Für den Komfort des automatisierten Stationensystems ist es wünschenswert wenn alle postalischen und Begleitscheinformulare auf eine oder eine limitierte Anzahl von Blankoformularen standardisiert werden kann.

Auffüllstation

Eine weitere Ausführungsform der Erfindung ist die Bereitstellung einer Benutzerkarten-Auffüllstation, die an irgendeinem postalischen Verkaufs- oder Verteilungsstandort unterhalten werden kann, für den Komfort des Erteilers von Karten und Benutzern. Eine neue Summe kann "aufgefüllt" werden, d.h. einem autorisierten Guthaben, das in der Benutzerkarte unterhalten wird, gutgeschrieben werden, und eine Hauptauffüllkarte, die eine größere Verteilungssumme hat, wird entsprechend belastet. In Übereinstimmung mit den Prinzipien der Erfindung wird die sichere Handshake-Erkennungsprozedur ausgeführt bevor die Transaktion autorisiert wird. Die Auffüllstation kann auch benutzt werden zum Gültigerklären von neu zu erteilenden Karten.

Eine exemplarische Ausführungsform der Auffüllstation ist in Fig. 10 gezeigt, die einen ersten Schlitz 161 für eine Hauptauffüllkarte 160 hat, einen zweiten Schlitz 171 für eine Überwachungskarte 170, einen dritten Schlitz 174 für eine Benutzerkarte 10, einen Stationenmikroprozessor 30", eine Tastatur 31" und eine Anzeige 32". Jede Karte ist von der zuvor beschriebenen Art, mit sicheren Mikroprozessoren (MPU) 162, 172 bzw. 60, die in Kontakt mit den entsprechenden Anschlußkontakten 163, 172 und 175 sind. Die Schalter 162, 172a und 176 stellen Erfassungssignale bereit, wenn die Karten in ihre entsprechenden Schlitz eingelegt sind. Der Betrieb der Stationen MPU 30" wird nach Einführung einer Hauptkarte 160 und einer Überwachungskarte 170 ermächtigt.

Eine Hauptauffüllkarte wird ursprünglich von einem zentralen Erteiler, wie beispielsweise dem U.S. Postdienst, einem autorisierten Verteiler für den zentralen Erteiler, oder einer privaten Überbringerfirma erworben. Es wird im allgemeinen beabsichtigt durch ein lokales Auffüllwesen erworben zu werden, das Dienste an individuelle Benutzer bereitstellt, wie beispielsweise einer Bankfiliale, einer Verkaufsstelle oder einer Corporationsabteilung. In der bevorzugten Ausführungsform wird sie in einer festen Einheit hergestellt und verbleibt verschlossen, bis sie von einer Überwachungskarte des zentralen Erteilers aktiviert wird. Die für die Handshake-Prozedur benutzten Verschlüsselungsalgorithmen sind bereits in ihre MPU "firmware" geschrieben, und ist ermächtigt die Handshake-Prozedur auszuführen, wenn die geheime Schlüsselzahl durch eine Überwachungskarte während der Aktivierungsprozedur installiert wird. Einmal aktiviert, wird das Guthaben der Hauptkarte für Auffülltransaktionen belastet, bis es aufgebraucht ist. Eine Vorgeschichte aller belastenden Transaktionen wird in der Hauptkarte aufrecht erhalten.

Eine Überwachungskarte wird von dem zentralen Erteiler unter Aufsicht eines Beamten oder Geschäftsführers des lokalen Auffüllwesens bereitgestellt, und eine Überwachungs PIN wird erteilt. Die Überwachungskarte wird zum Entriegeln aller Hauptkarten, die an das Auffüllwesen verkauft wurden, benutzt, und zum Aufrechterhalten einer Aufzeichnung der Seriennummern der Hauptkarten für nachfolgende Kartenbestätigungs-Prozeduren. Sie wird zum Autorisieren von Gutschreibetransaktionen an Benutzerkarten benutzt, und unterhält eine Transaktionsaufzeichnung aller Auffülloperationen und die Identität von Empfängerbenutzerkarten. Die Überwachungskarte wird mit dem Handshake-Verschlüsselungsalgorithmen in "firmware" hergestellt, und kann von dem

zentralen Erteiler mit geheimer Schlüsselzahl ausgestattet werden, um in den Haupt- und Benutzerkarten installiert zu werden. Die Haupt- und Überwachungskarten erlauben zusammen, daß Benutzerkarten bequem an weitverbreiteten lokalen Wesen aufgefüllt werden, ohne den Bedarf einer "on-line"-Bestätigung jeder Auffülltransaktion durch den zentralen Erteiler. Alternativ kann die Benutzerkarte durch die Hauptkarte alleine aufgefüllt werden, wobei die Handshake-Prozedur zwischen der Benutzerkarten MPU und der Hauptkarten MPU ausgeführt wird. Jedoch wird der Gebrauch einer Steuerungsüberwachungskarte als eine zusätzliche Sicherheitsstufe bevorzugt, um Fälschen oder betrügerischen Gebrauch von Hauptkarten mit höherem Wert zu verhindern.

Der Betrieb der Auffüllstation soll nun für die bevorzugte Drei-Karten-Ausführungsform, mit Bezug auf das Blockdiagramm von Fig. 11, beschrieben werden. Nach Initiieren der Stationprogramms wird die Hauptkarte bei Block 180 geprüft, um festzustellen, ob sie schon aktiviert ist. Falls nicht, folgt die Station eine Aktivierungsprozedur bei Block 181 zum Bestätigen der Überwachungs PIN, Prüfen der Hauptkartenseriennummer, Installieren einer geheimen Schlüsselzahl in der Hauptkarte, Ausführen der Handshake-Prozedur, dann Entriegeln des Guthabens der Hauptkarte und Aufzeichnen der Seriennummer, Guthabens, Datums und anderen Transaktionsinformationen.

Wenn die Hauptkarte schon aktiviert worden ist, vergleicht die Überwachungskarte die Seriennummer der Hauptkarte mit ihrer Aufzeichnung von autorisierten Hauptkarten. Wenn die Hauptkarte nicht autorisiert ist geht das Stationenprogramm zu einer Endprozedur bei Block 790 über. Mit einer autorisierten Hauptkarte prüft das Stationenprogramm, ob die in die Station eingeführte Benutzerkarte neu ist oder aufgefüllt werden soll. Für eine neue Benutzerkarte führt die Auffüllstation bei Blöcken 190-193 eine Gültigkeitsprozedur aus, die ein Vergleichen der anderen Kartenseriennummer mit der in ihrem Speicher eingelassenen Nummer, ein Aufzeichnen der Benutzeridentifikationsinformation und ein Zuordnen einer Benutzer PIN umfaßt. Bei Block 192 fragt die Station den Bediener nach irgendwelchen Einschränkungen der Summen oder Art von Transaktionen für die die Karte benutzt werden kann, den Identifikationsnummern der Stationen, zu denen die Karte beschränkt ist, oder einem Ablaufdatum, wenn von dem Erteiler benötigt. Die Gültigkeitsprozedur wird durch Installieren der geheimen Schlüsselzahl und Versiegeln der geheimen Speicherzone abgeschlossen.

Wenn die Benutzerkarte aufgefüllt werden soll wird die Benutzer PIN bestätigt, und die Karte wird dann auf irgendein Guthaben hin, das der neuen Summe oder dem Benutzerkonto gutgeschrieben werden soll, geprüft. Der alte Speicherabschnitt wird dann für weitere Transaktionen verriegelt und kann nur zum Auslesen einer Transaktionsvorgeschichte benutzt werden. Nach einer Anfrage für eine neue Summe, entweder für eine neue Karte, die für gültig erklärt worden ist, oder für eine aufzufüllende Karte, öffnet die Stationen MPU 30" einen Handshake-Kanal, und die zuvor beschriebene Handshake-Prozedur wird zwischen der Haupt MPU 172 und der Überwachungs MPU 172 ausgeführt. Wenn die Handshake-Prozedur abgeschlossen ist wird das Hauptgutachten belastet und die Überwachungskarte fährt fort einen neuen Transaktionsspeicherabschnitt in der Benutzerkarte zu öffnen, in die das neue Guthaben geschrieben wird. Das Programm stellt dann bei Block 197 eine Endauswahl für weitere Operationen bereit, die an der Auffüllstation ausgeführt werden können. Zum Beispiel kann eine andere Auffülltransaktion bearbeitet werden, die Überwachungskartenaufzeichnung kann aktualisiert werden, den neu für gültig erklärten Benutzer- oder Hauptkarten kann eine Seriennummer oder Kontonummer eingeprägt werden, wenn die Station mit einer Prägemaschine verbunden ist, oder Funktionsweisen können abgeschlossen werden.

Das beschriebene Auffüllsystem ist an mehreren Sicherheitsstufen geschützt. Erstens wird eine Überwachungskarte benötigt und die Benutzerkarte muß mit einer Benutzer PIN für gültig erklärt werden. Die Hauptkarte muß durch die Überwachungskarte für gültig erklärt werden und muß die Handshake-Prozedur ausführen, bevor der Benutzerkarte eine neue Summe gutgeschrieben wird. Das Karten/Stationensystem hat den wesentlichen Vorteil, daß das Belasten des Kartenguthabens in dem gleichen Zeitrahmen ausgeführt wird da der Wertausgabebetrieb ausgeführt wird, und der Austausch kann für jede Transaktion nur ausgeführt werden, wenn die gegenseitige Handshake-Erkennungsprozedur zwischen den sicheren Gruppen, die jeden Teil steuern, ausgeführt wird. Der zentrale Erteiler erwirbt das Karten/Stationensystem von dem Hersteller auch mit einem gegebenen Satz von Verschlüsselungsalgorithmen, und wählt dann einen einzigartigen geheimen Schlüssel aus, der dem Hersteller nicht bekannt ist. Somit wird eine Durchdringung der Sicherheit des Herstellers die Sicherheit des Erteilersystems nicht gefährden. Durch Erteilung von Karten mit definierten Ablaufdaten oder Seriennummern, und durch periodisches Ändern des geheimen

Schlüssels kann ein Erteilersystem noch undurchdringbarer für Fälscher gemacht werden.

Die Benutzerkarte ist nicht nur eine passive Aufzeichnung einer Kontonummer und eines Guthabens, sondern arbeitet zum positiven Schutz gegen nicht autorisierten Gebrauch von Karten, z.B. wenn eine Serie von inkorrekten PIN Eingaben gemacht wird, wenn in die Karte über ihr Ablaufdatum hinaus oder in einer nicht autorisierten Maschine gebraucht wird, oder wenn eine verlangte Transaktion vorgegebene Grenzen überschreitet. In ähnlicher Weise ist der wertausgebende Teil der Station gegen Manipulation geschützt, durch die körperliche Verbindung des Druckermikroprozessors mit dem Druckkopf.

Des weiteren, da die postalischen und Auffülltransaktionen mit Karten ausgeführt werden, die von einem zentralen Erteiler ausgeteilt werden, und nur innerhalb des Systems des Erteilers stattfinden, sind sie gegen gefälschte Karten oder Karten geschützt, die von einem anderen System ausgegeben wurden. Somit verbleibt ein Erteilersystem für alle anderen Erteilersysteme geschlossen, und mehrere Systeme können die gleichen Stationen benutzen, ohne Störung durch ein anderes. Zum Beispiel kann der U.S. Postdienst und mehrere private Überbringer jeweils ein getrenntes Erteilersystem bilden, das seine eigenen Karten erteilt. Ein Benutzer kann eine Karte von jedem System beziehen und die richtige Karte in irgendeiner Station verwenden, die an einem lokalen Wesen (Postamtfiliale, Bankfiliale, lokale Verkaufsstelle) unterhalten wird, um ein autorisiertes Porto oder einen Begleitschein zum Gebrauch in dem entsprechenden System zu erzeugen. Somit werden Benutzer den Vorteil von sicherem und bequemem Zugriff auf eine weite Reihe von postalischen und Überbringerdiensten haben.

In dem System umfassen die Mikroprozessorkarten (Benutzer, Haupt- und Überwachung), Speicherkarten (Gebühren und Sonderdienste) und Stationen (Zumessen, Begleitscheindrucken und Auffüllen) ein integriertes postalisches Transaktionssystem, das einen stark verbesserten Grad an Zugriff, Bequemlichkeit und Sicherheit bereitstellt, im Vergleich zu herkömmlichen postalischen Maschinen. Das gesamte System ist in Fig. 12 dargestellt. Es erlaubt, daß weitverteilte Benutzerkarten in weit verbreiteten Postzumeß- und Begleitschein-Druckstationen benutzt werden können, mit den passenden Gebühren und/oder Dienstkarten, um auf eine Vielzahl von Post- und Überbringerdiensten zugreifen zu können. Die Auffüllstationen erlauben einem zentralen Erteiler postalische Geldwerte an Benutzer an weit verbreiteten Standorten zu verteilen. Strikte körperliche

Zugriffskontrollen werden nicht benötigt, der Bedarf die postalischen Summen und Dienste, die durch die erteilten Karten erhältlich sind, zu limitieren ist reduziert, persönliche Kauftransaktionen werden vermieden, und eine "on-line"-Bestätigung durch einen zentralen Kontobeamten wird vermieden. Die Karten und Stationen sind konfiguriert autonom zu sein, dennoch werden gegenseitige Erkennung und Bestätigung von Gültigkeits- und Transaktionssummen benötigt, wodurch ein hoher Grad an Sicherheit für das System bereitgestellt wird.

Des weiteren ist die Erfindung nicht auf die beschriebenen automatisierten postalischen Stationen limitiert. Die Prinzipien der Erfindung können auf irgendeine andere wertaustauschende Transaktion angewendet werden, wo gewünscht wird eine Kontokarte in einem "off-line"-automatisierten Stationensystem zu verwenden. Somit können die beschriebenen intelligenten Karten ("smart cards") und wertausgebenden Stationen auch zum Ausgeben von Bargeld, Drucken von Eintrittskarten, Erteilen von Coupons etc. benutzt werden, und der Benutzer kann eine Vielfalt an Karten besitzen, wobei jede durch einen zentralen Erteiler für den bequemen Erwerb von verschiedenen Wertgegenständen ausgegeben wird. Durch Implementieren von "smart card" und Stationen MPU Programmen, die autorisierte Maschinenidentifikationsnummern und Kartenseriennummern prüfen, oder die Handshake-Prozedur mit verschiedenen Algorithmen und/oder geheimen Schlüsseln ausführen, kann ein Erteilersystem konfiguriert werden, so daß die Erteilerkarten und Stationen für bestimmte Familien, Serien oder Standorte geöffnet oder eingeschränkt werden können.

Das System umfaßt auch andere Kennzeichen, die nützliche Anhängsel für das oben beschriebene zentrale Konzept sind. Zum Beispiel kann ein Transaktions-Vorgeschichten-Drucker bereitgestellt werden, von dem ein Benutzer eine Aufzeichnung von Transaktionen drucken kann, die in der "smart card" nach Eingabe der korrekten PIN gespeichert wird. Die verschiedenen Karten können mit Kerben an einem Grenz- oder codierten Schlüsselement ausgestattet sein, um ein Einführen der falschen Karte in einen inkorrekten Stationenschlitz oder in eine Station eines anderen Erteilersystems zu verhindern. Das System kann auch für "on-line"-Transaktionssysteme angepaßt werden. Zum Beispiel kann die Stationen MPU durch eine Telefonleitung oder ein lokales Netzwerk an ein zentrales Verarbeitungsbüro angeschlossen werden, zum Bestätigen einer Transaktion vor dem Ausführen der Transaktion. "On-line"-Bestätigung kann für Initialisierungs- und Auffülltransaktionen erwünscht werden, die weniger

häufig und von höherem Wert als Kauftransaktionen sind. Als weiteres Sicherheitskennzeichen kann die Karte oder Serien von Karten mit Verschlüsselungsalgorithmen und/oder geheimen Schlüsselzahlen ausgegeben werden, die periodisch geändert werden, und die Verschlüsselungsalgorithmen und geheimen Schlüssel, die Karten entsprechen, die für eine Transaktion präsentiert werden, können in die Station geladen werden zu dem Zeitpunkt, da die Stationen MPU eine "on-line"-Verbindung mit dem zentralen Büro herstellt.

Innerhalb des Rahmens der Erfindung kann das zuvor beschriebene interaktive kartenautomatisierte Transaktionssystem auf Portozumeßmaschinen angewendet werden. In einer Ausführungsform hat eine Portozumeßstation einen Schlitz zum Aufnehmen einer Mikroprozessorkarte, die mit einem autorisierten Guthaben erteilt wird, einen Druckkopf mit einem sicheren Mikroprozessor, der mit dem Kartenmikroprozessor wechselwirkt, ein Eingabefeld, eine Anzeige und einen Betriebsmikroprozessor, der eine verschlüsselte Eingabe des verlangten Portowertes akzeptiert, die verschlüsselte Eingabe anzeigt, die Karte abfragt die Portodrucktransaktion zu autorisieren und zu initiieren und dann die Maschine für die nächste Transaktion zurücksetzt oder eine Reihe von Transaktionen in einem Wiederholungsmodus ausführt.

In einer verwandten Ausführungsform hat eine Portozumeßstation einen ersten Schlitz zur Aufnahme einer Benutzermikroprozessorkarte, einen zweiten Schlitz zur Aufnahme einer postalischen Gebührenkarte, einen Druckkopf mit einem sicheren Mikroprozessor, ein Eingabefeld und andere Einrichtungen zur Eingabe von Ursprungs- und Bestimmungspostleitzahlen, Einrichtungen zur Eingabe des Gewichts und Postkategorie des zu versendenden Gegenstandes, und einen Betriebsmikroprozessor, der ein Programm zum Berechnen des richtigen Portos hat, basierend auf den Auflistungen der Gebührenkarte und den eingegebenen Informationen.

Das kartenautomatisierte postalische Transaktionssystem kann nicht nur leicht auf die postalischen Produkte und Dienste des U.S. Postdienstes angewendet werden, sondern auch auf private Überbringer und Paketlieferungsfirmen. In einer weiteren Ausführungsform hat eine postalische Belegscheinstation einen dritten Schlitz zur Aufnahme einer speziellen Dienstkarte, die gespeicherte Daten hat, von der die Station postalische und Lieferdienstinformation auf Standardblankoformulare drucken kann. Zum Beispiel kann die Sonderdienstkarte benutzt werden, um Postamtformulare zu drucken, wie beispielsweise beglaubigte Post oder

eingeschriebene Post, oder die Begleitscheine von privaten Überbringerfirmen. Die Station ist auch mit einer Gesamtbereichsanzeige des Begleitscheinformulars ausgestattet, fragt den Benutzer nach Information mittels programmierter Zeigerbewegungen, und hat Befehlstasten zur Eingabe von Absender und Empfängerinformation, Gebühren oder Leistungskategorie, Begleitscheinnummer, Überbringerinformation, etc..

Als untergeordnete Kennzeichen können die Mikroprozessorkarten konfiguriert werden, um verschiedene Zugriffsarten auf die Stationen wie gewünscht bereitzustellen, z.B. limitierte Anzahlen oder Arten von Benutzern in limitierten Anzahlen oder Typen von Maschinen, nichtlimitierte Benutzer in limitierten Maschinen, limitierte Benutzer in nichtlimitierten Maschinen oder nichtlimitierte Benutzer in nichtlimitierten Maschinen. Die verschiedenen Zugriffsarten können durch Speichern von Schlüsselzahlen in der Karte ausgeführt werden, zum Identifizieren autorisierter Benutzer und/oder Maschinen, und/oder durch Schlüsselzahlen in dem Betriebsmikroprozessor der Station, zum Identifizieren autorisierter Benutzer. Die Benutzerkarten können auch zum Zeitpunkt der Erteilung konfiguriert werden, zum Limitieren der Summen und Arten individueller Transaktionen, und zum vorübergehenden oder permanenten Verriegeln nach Erfassen eines nicht autorisierten Benutzers oder Karte. Ein anderes Kennzeichen des Systems ist das Speichern einer durch die Karte ausgeführten Transaktionsvorgeschichte und das Wiederberechnen des verbleibenden Guthabens nach jeder verlangten Transaktion, um Kartenspeicherplatz zu sparen. Ein separater Transaktionsdrucker kann benutzt werden, um einen Ausdruck der Transaktionsvorgeschichte der Karte zu erhalten.

Die Portozumeßstationen können auch mit Einrichtungen ausgestattet sein, um einem Postamt oder Überbringer zu erlauben die gedruckten Portomarkierungen oder Begleitscheine zu beglaubigen. In einer Ausführungsform druckt der Stationendrucker innerhalb oder unter den Portostempel eine codierte Zahl oder eine Sequenz von Markierungen, die einem Element des Portostempels entsprechen, wie beispielsweise die Summe des Portos, die Stationsidentifikationsnummer und/oder die Postleitzahl des Absenders. Die Markierungen können verschleiert oder unsichtbar gemacht werden, durch Drucken mit einer magnetisch oder optisch lesbaren Tinte, um Manipulation oder nicht autorisierte Nachahmung abzuschrecken. Sie können dann für das Postamt oder eine private Überbringerfirma lesbar sein, um festzustellen, ob der gedruckte Portostempel von einem autorisierten

Drucker gedruckt wurde, und gleichzeitig wird ein Prüfstreifen an den Absender bereitgestellt.

Gemäß einer weiteren Anwendung der Erfindung kann ein integriertes System von Mikroprozessorkarten und Stationen Transaktionseinrichtungen bereitstellen, die weit verbreiteten Gebrauch und bequemen Zugriff für Benutzer erlauben. Die autorisierte Summe der Benutzerkarte kann anfänglich für gültig erklärt werden oder von einer Hauptauffüllkarte, die eine größere autorisierte Summe hat, aufgefüllt werden, vorzugsweise in Verbindung mit einer Überwachungskarte, die unter strikter Verteilungskontrolle erteilt wird. Eine Auffüllstation ist mit drei Einführschlitzen für drei Karten ausgestattet, und hat ein Betriebsprogramm zum Überprüfen der Identität der Hauptauffüllkarte und der Benutzerkarte, um festzustellen, ob sie für einen Gebrauch in der Auffüllstation gültig sind. Nach Leerung muß die sichere Handshake-Erkennungsprozedur erfolgreich zwischen den Mikroprozessoren der Überwachungs- und Hauptkarten ausgeführt werden, um ein Belasten der Hauptkarte über die Auffüllsumme, und ein Gutschreiben für die Benutzerkarte zu erlauben. Wenn die Benutzerkarte eine neue Karte ist, werden eine Gültigkeitsprozedur und das Auswählen und Speichern einer Benutzer PIN ausgeführt.

Das kartenautomatisierte Transaktionssystem der Erfindung hat eine breite Anwendbarkeit auf viele andere Arten von Verkaufs- oder Kredittransaktionen neben postalischen Dienste und Produkten. Zum Beispiel kann es auch für Kreditkartentransaktionen, Lagerbestandskontrolle, Frachtrechnungen, automatisierte Bargeldautomaten oder praktisch irgendeine andere Transaktionsart in der ein Benutzerkonto sicher über eine automatisierte Station belastet werden muß, in Austausch eines Gegenstandes oder Wertartikels benutzt werden. Die Erfindung ist insbesondere vorteilhaft in "off-line" Transaktionen, in denen verteilte Stationen, die nicht unter strikten Zugriffskontrollen sind, benutzt werden.

Basierend auf der vorangegangenen Offenbarung werden viele andere peripherischen Kennzeichen und Modifikationen und Variationen der Prinzipien der Erfindung Personen offensichtlich werden, die mit automatisierten Stationen und "smart card"-Systemen vertraut sind. Es ist beabsichtigt, daß die hier beschriebenen Ausführungsformen und Kennzeichen und alle anderen Kennzeichen, Modifikationen und Variationen in dem erlaubten Anwendungsbereich der Erfindung beinhaltet sind, wie in den anhängenden Ansprüchen definiert.

P a t e n t a n s p r ü c h e

1. Ein automatisiertes Transaktionssystem, umfassend eine Transaktionsstation (20) mit einem Aufnahmeschlitz (11), um darin eine tragbare Benutzerkarte (10) durch einen Benutzer einzuführen, einen Betriebsabschnitt (30) in der Station (20) zum Ausführen von Stationsfunktionen, einschließlich der Funktion einer Transaktion eines Wertartikels durch die Station, und eine Eingabeeinrichtung (31), die mit der Station (20) verbunden ist, um einem Benutzer zu erlauben, eine Nachfrage für einen Wertartikel, der durch die Station durchzuführen ist, einzugeben, wobei:

eine Mehrzahl von tragbaren Gebührenkarten vorgesehen ist, von denen jede Gebührenkarte (90) einen Speicher (92) darin eingebettet zum Speichern von Gebühreninformation, die einer entsprechenden der Mehrzahl von verschiedenen durch die Station durchzuführende Transaktionsdiensten entspricht, und eine Datenausgabeeinrichtung (93) hat, die mit dem Speicher verbunden ist;

ein zweiter Aufnahmeschlitz (91) in der Station zur Aufnahme der Gebührenkarten (90) vorgesehen ist;

die Station Verbindungsleitungen zum Herstellen einer Verbindung zwischen ihrem Betriebsabschnitt (30) und der Datenausgabeeinrichtung (93) der Gebührenkarte (90) umfaßt, die in den zweiten Aufnahmeschlitz (91) in der Station eingeführt ist

der Betriebsabschnitt (30) der Station ein gespeichertes Programm zum Ausführen einer Verifizierungsprozedur zum Verifizieren, daß eine durch den Benutzer eingeführte Gebührenkarte einem ausgewählten Transaktionsdienst entspricht, für die ein Wertartikel verlangt wird, und eine Gebührenberechnungsprozedur umfaßt zum Berechnen des Transaktionsdienstwerts des verlangten Artikels, unter der Verwendung der in dem Speicher (92) der eingeführten Gebührenkarte (90) gespeicherten Gebühreninformation; und

ein Wertausgabeabschnitt (40) mit der Station (20) vorgesehen ist, zur Ausgabe eines verlangten Artikels des ausgewählten Transaktionsdienst, in Übereinstimmung mit dem Transaktionsdienstwert, der in der durch den Betriebsabschnitt (30) der Station ausgeführten Gebührenberechnungsprozedur

berechnet wird, der betreibbar ist zu veranlassen, daß der Transaktionsdienstwert in der Benutzerkarte (10) aufgezeichnet wird.

2. Ein automatisiertes Transaktionssystem nach Anspruch 1, dadurch gekennzeichnet, daß der Betriebsabschnitt (30) der Station einen Betriebsmikroprozessor umfaßt, der mit Gebühreninformation von dem Speicher der eingeführten Gebührenkarte für einen ausgewählten Transaktionsdienst geladen wird.

3. Ein automatisiertes Transaktionssystem nach Anspruch 1, dadurch gekennzeichnet, daß der auszugebende Wertartikel ein gedrucktes Wertzeichen ist, hinweisend auf den von dem Benutzer verlangten Artikel, und die Station (20) einen Drucker als den wertausgebenden Abschnitt (40) zum Drucken des Wertzeichens auf einen Artikel umfaßt

4. Ein automatisiertes Transaktionssystem nach Anspruch 3, dadurch gekennzeichnet, daß die Mehrzahl von verschiedenen Transaktionsdiensten postalische Dienste sind, die von verschiedenen postalischen Unternehmern bereitgestellt werden, und daß das gedruckte Wertzeichen ein Portostempel ist, der mit einem entsprechenden der Mehrzahl von verschiedenen postalischen Unternehmern assoziiert ist.

5. Ein automatisiertes Transaktionssystem nach Anspruch 3, dadurch gekennzeichnet, daß der Speicher der tragbaren Gebührenkarten auch zum Speichern und Laden von graphischen Daten benützt wird zum Erzeugen eines besonderen Wertzeichens, das für einen entsprechenden postalischen Unternehmer gedruckt werden soll.

6. Ein automatisiertes Transaktionssystem nach Anspruch 3, weiter gekennzeichnet durch eine Waage (53) zum Wiegen eines Gegenstandes und zum Erzeugen eines Signals, das auf dessen Gewicht hinweist, wobei die Waage mit der Station verbunden ist, um das Wiegesignal an den Betriebsabschnitt (30) der Station zu liefern, zum Berechnen der postalischen Wertsumme für ein ausgewähltes postalisches Unternehmen, unter Verwendung der in dem Speicher der eingeführten Gebührenkarte gespeicherten Gebühreninformation.

7. Ein automatisiertes Transaktionssystem, umfassend eine Transaktionsstation (20) mit einem Aufnahmeschlitz (11), um darin durch einen Benutzer eine tragbare Benutzerkarte (10) einzuführen, und einen Betriebsabschnitt (30) in der Station (20) zum Ausführen von Stationsfunktionen, einschließlich der Funktion einer Transaktion eines Wertartikels durch die Station, wobei:

eine Mehrzahl von tragbaren Dienstkarten (100) vorgesehen ist, von denen jede Dienstkarte (100) einen Speicher (102) darin eingebettet, zum

Speichern von Dienstsntprogramminformation, die einer entsprechenden der Mehrzahl von verschiedenen durch die Station durchzuführenden Diensten entspricht, und eine Datenausgabeeinrichtung (103) hat, die mit dem Speicher verbunden ist;

ein zweiter Aufnahmeschlitz (101) in der Station vorgesehen ist, zum Aufnehmen der Dienstkarten (100);

die Station (20) Verbindungsleitungen, zum Herstellen einer Verbindung zwischen ihrem Betriebsabschnitt (30) und der Datenausgabeeinrichtung (103) einer Dienstkarte (100) umfaßt, die in den zweiten Aufnahmeschlitz (101) in der Station eingeführt ist;

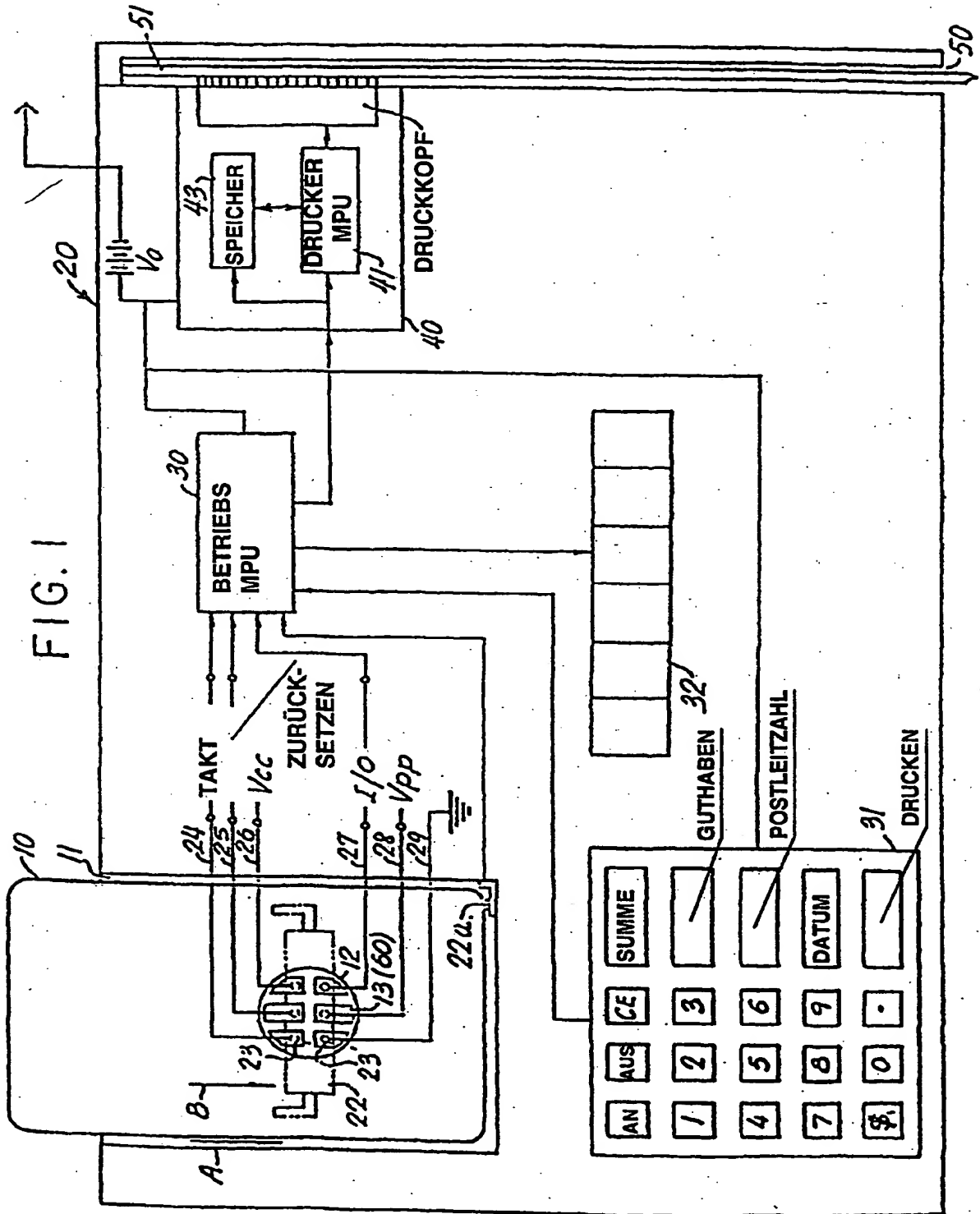
der Betriebsabschnitt (30) der Station (20) ein gespeichertes Programm umfaßt, zum Ausführen einer Verifizierungsprozedur zum Verifizieren, daß eine durch den Benutzer eingeführte Dienstkarte einem ausgewählten Transaktionsdienst entspricht, für die ein Wertartikel verlangt wird, und einer Dienstprogramm-Benutzungsprozedur zum Benutzen des in dem Speicher (102) der eingeführten Dienstkarte (100) gespeicherten Transaktionsdienstprogramms; und

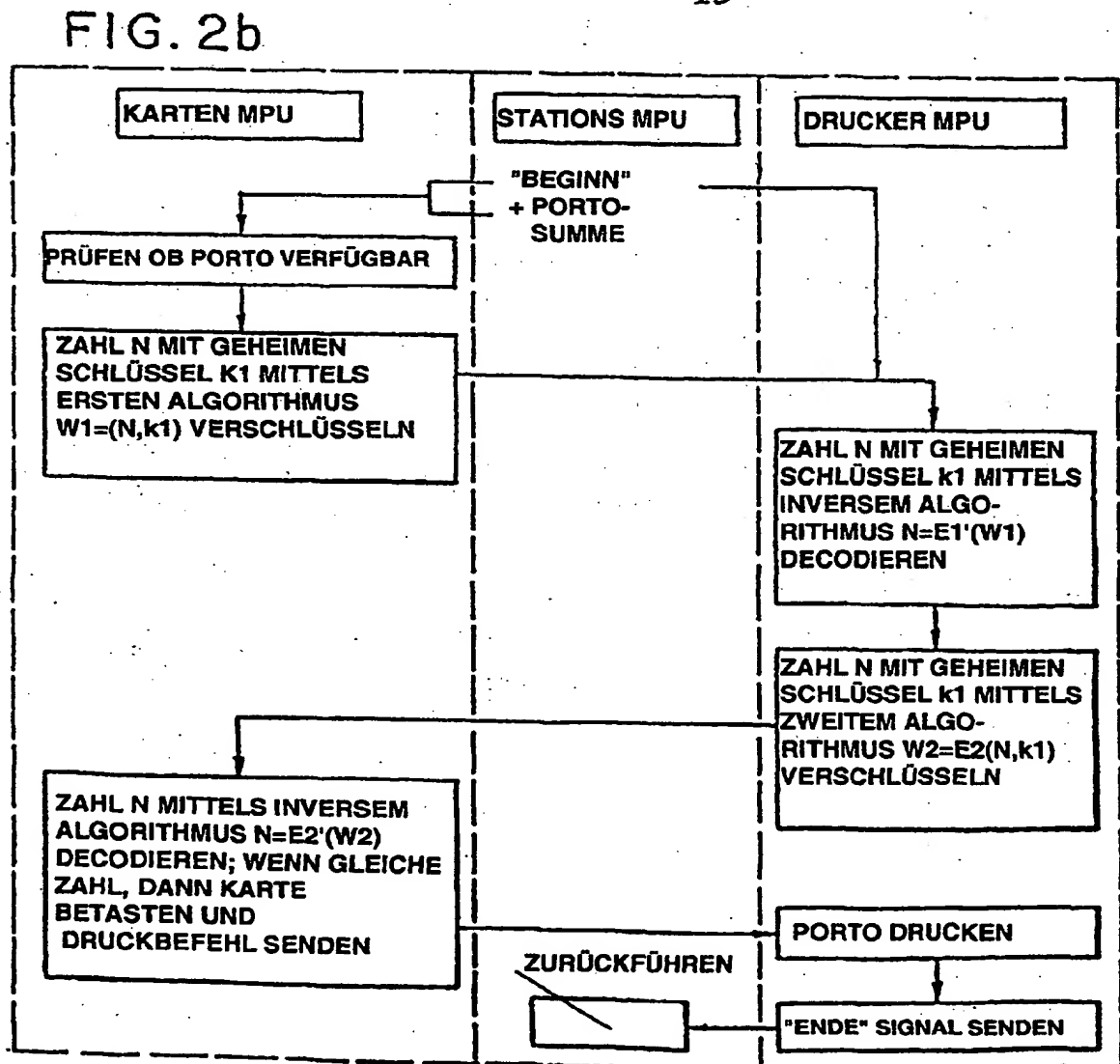
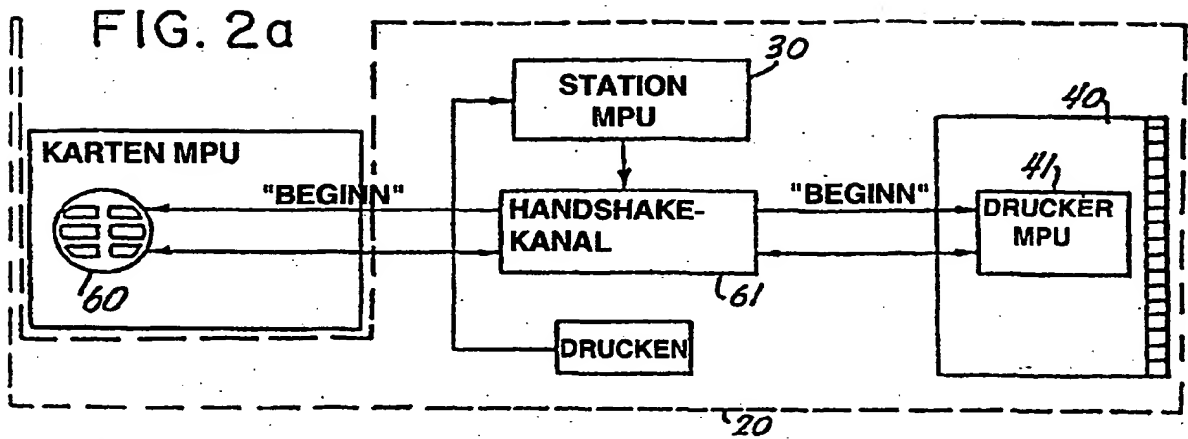
ein Wertausgabeabschnitt (40) mit der Station (20) vorgesehen ist, zur Ausgabe eines verlangten Artikels des ausgewählten Transaktionsdienstes, in Übereinstimmung mit dem Transaktionsdienstprogramm, das von dem Betriebsabschnitt (30) der Station benutzt wird, der weiterhin betreibbar ist, um den Transaktionsdienstwert zu berechnen, und veranlaßt, daß er in der Benutzerkarte (10) aufgezeichnet wird.

8. Ein automatisiertes Transaktionssystem nach Anspruch 7, dadurch gekennzeichnet, daß der Betriebsabschnitt (30) der Station (20) einen Betriebsmikroprozessor umfaßt, der mit der Dienstprogramminformation von dem Speicher der eingeführten Dienstkarte für einen ausgewählten Transaktionsdienst geladen wird..

9. Ein automatisiertes Transaktionssystem nach Anspruch 7, dadurch gekennzeichnet, daß der auszugebende Wertartikel eine gedruckte Aufzeichnung ist, hinweisend auf einen durch den Benutzer verlangten Artikel von dem ausgewählten Transaktionsdienst, und die Station einen Drucker als den wertausgebenden Abschnitt (40) zum Drucken der gedruckten Aufzeichnung umfaßt.

10. Ein automatisiertes Transaktionssystem nach Anspruch 9, dadurch gekennzeichnet, daß eine Mehrzahl von verschiedenen Transaktionsdiensten verschiedene postalische Dienste sind, und die zu druckende Aufzeichnung ein Begleitschein ist, der einem ausgewählten postalischen Dienst zugeordnet ist.





SICHERHEITS- STUFE	I	II	III	IV
-----------------------	---	----	-----	----

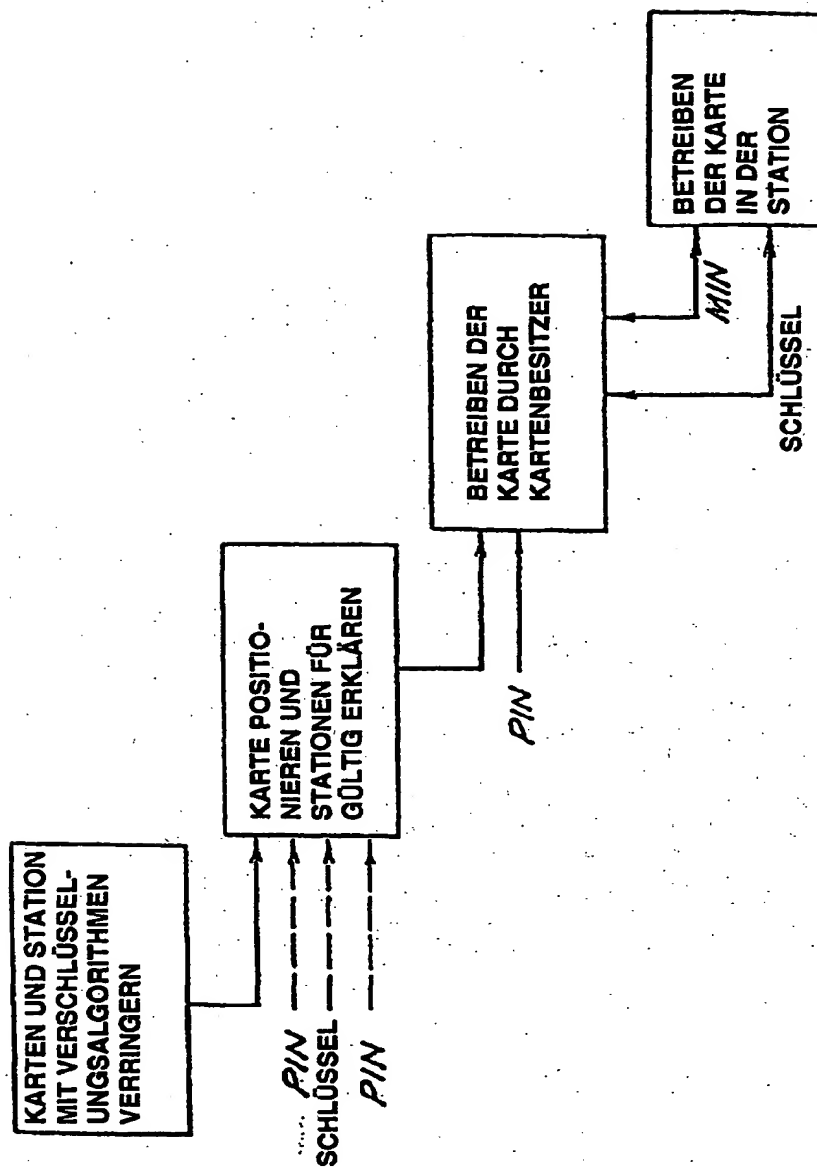


FIG. 3

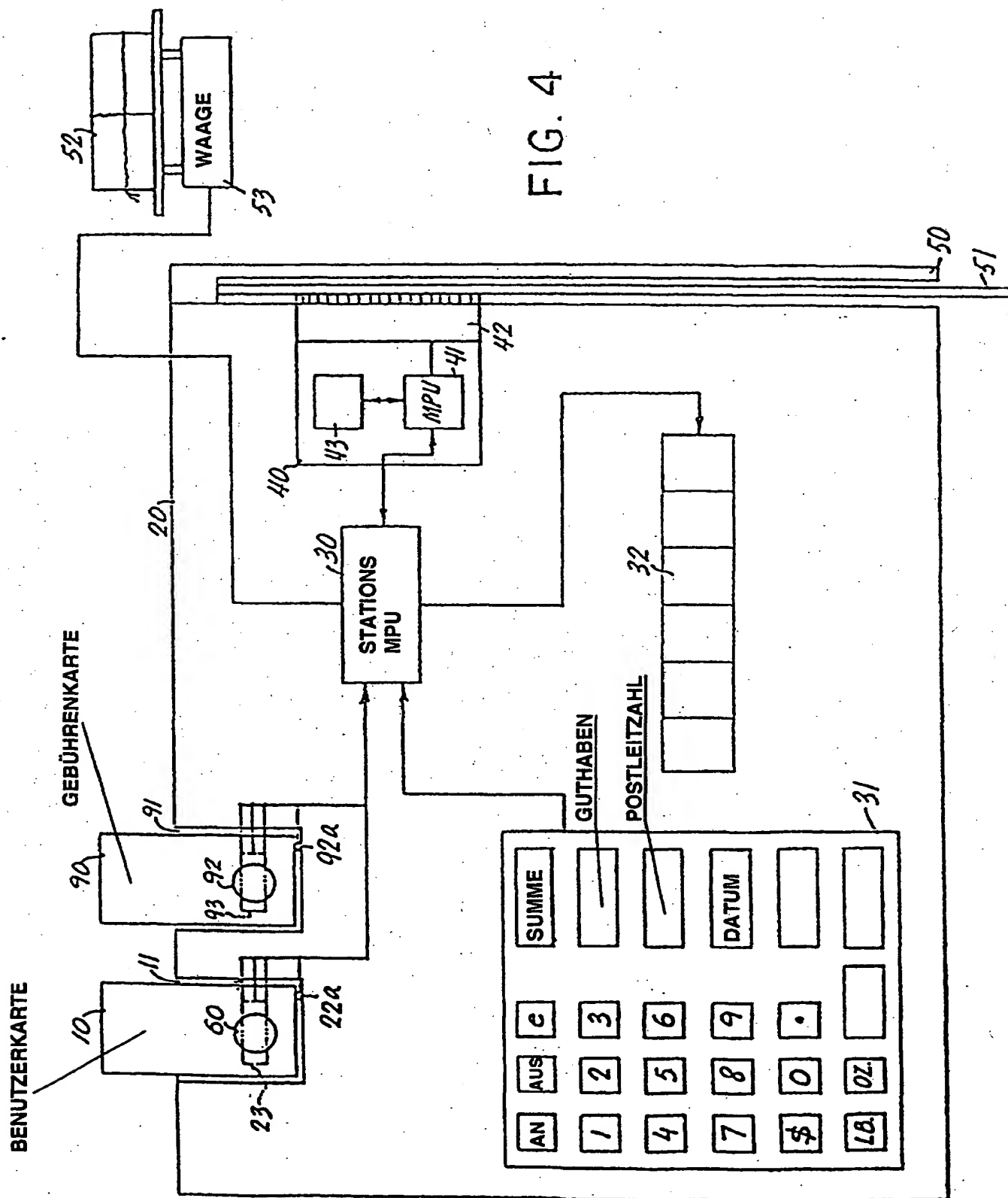
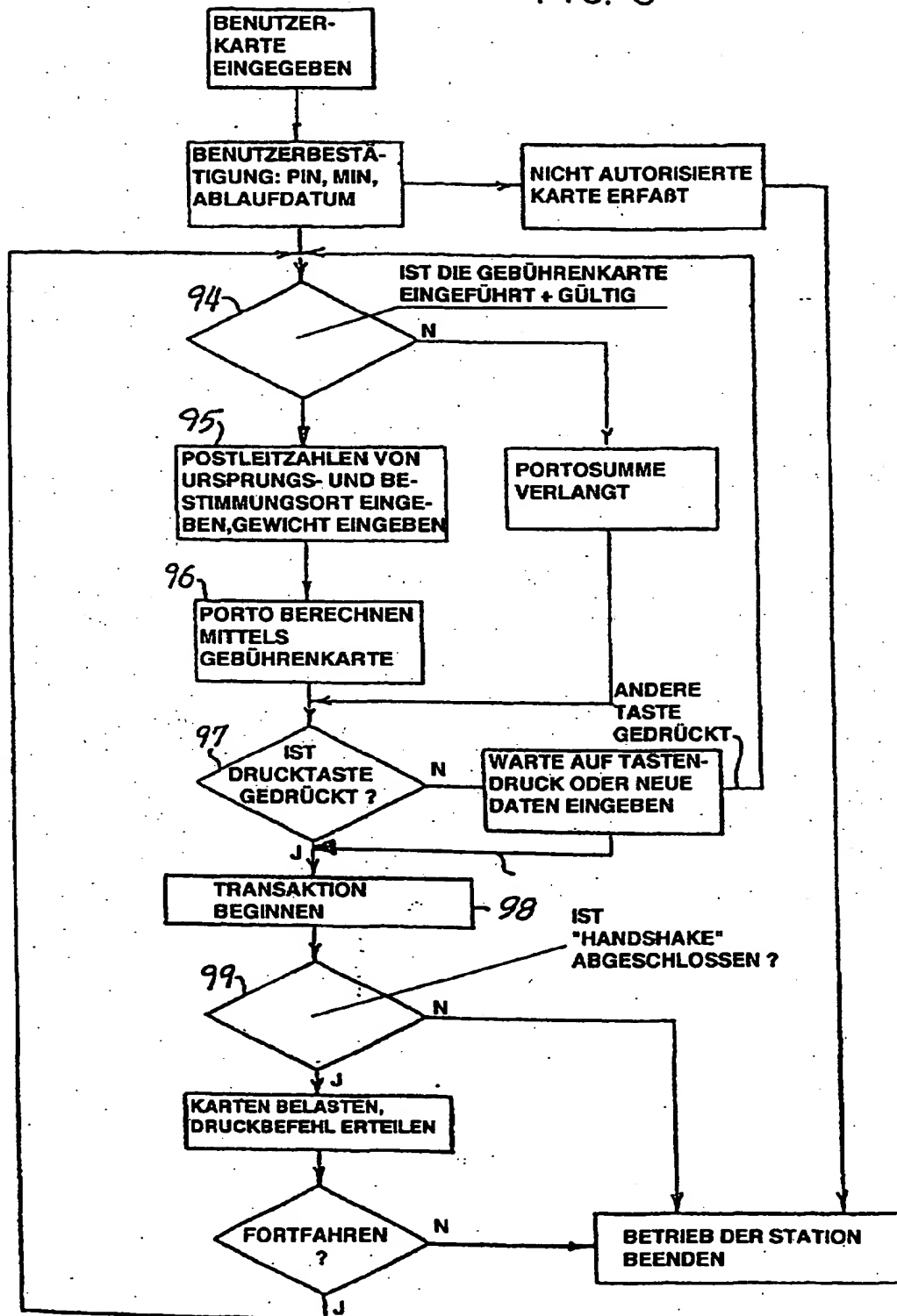


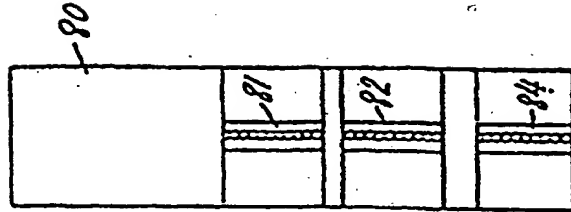
FIG. 4

27.11.97

5/11

FIG. 5





BIT	1	2	3	4	5	6	7	8	9	0
I	•		•		•		•		•	
II		•	•			•	•			
III				•	•	•	•			
IV								•	•	

FIG. 6b

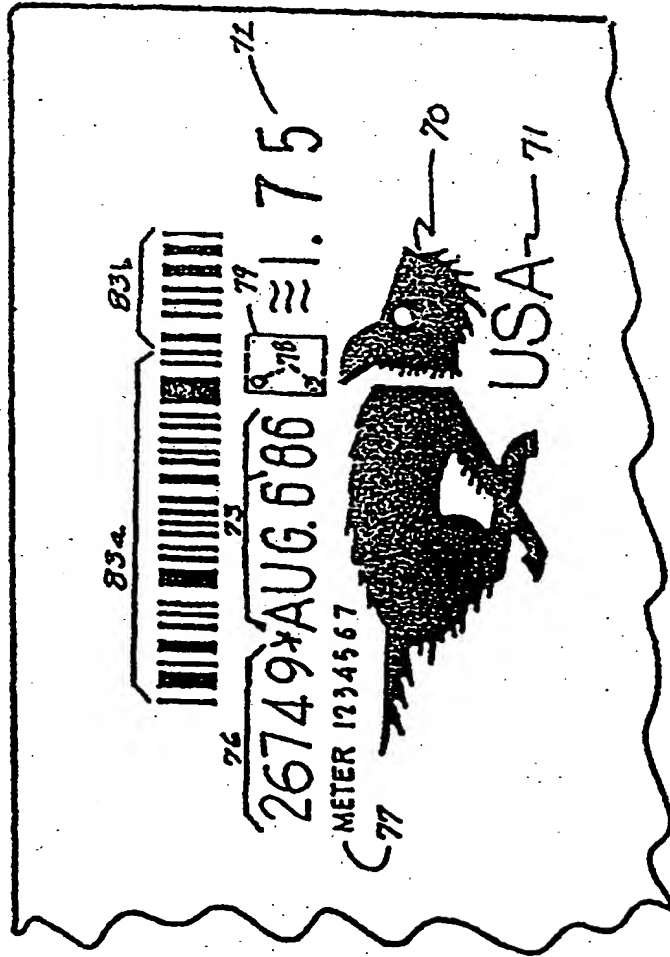


FIG. 6a

27.11.97

7/11

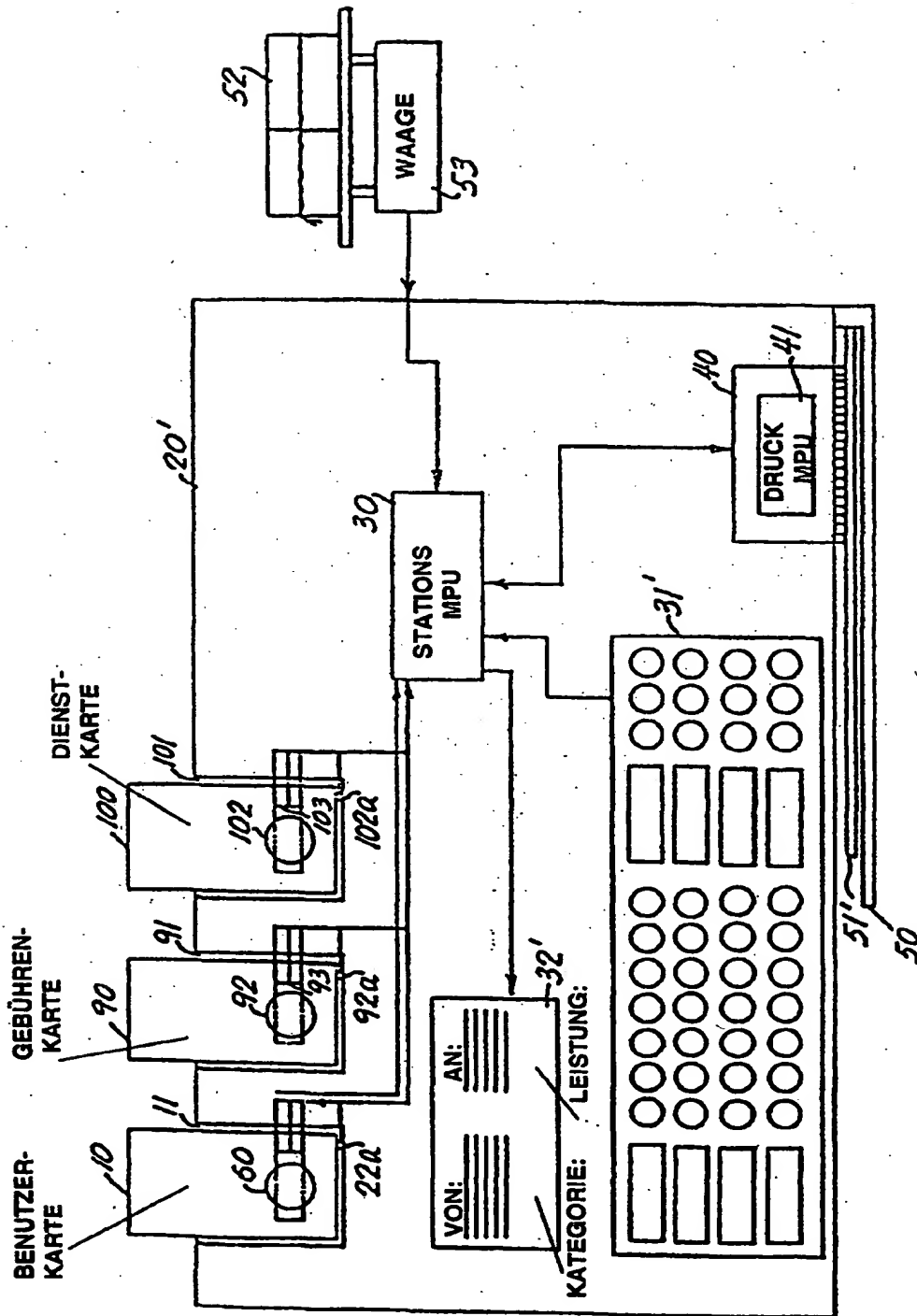
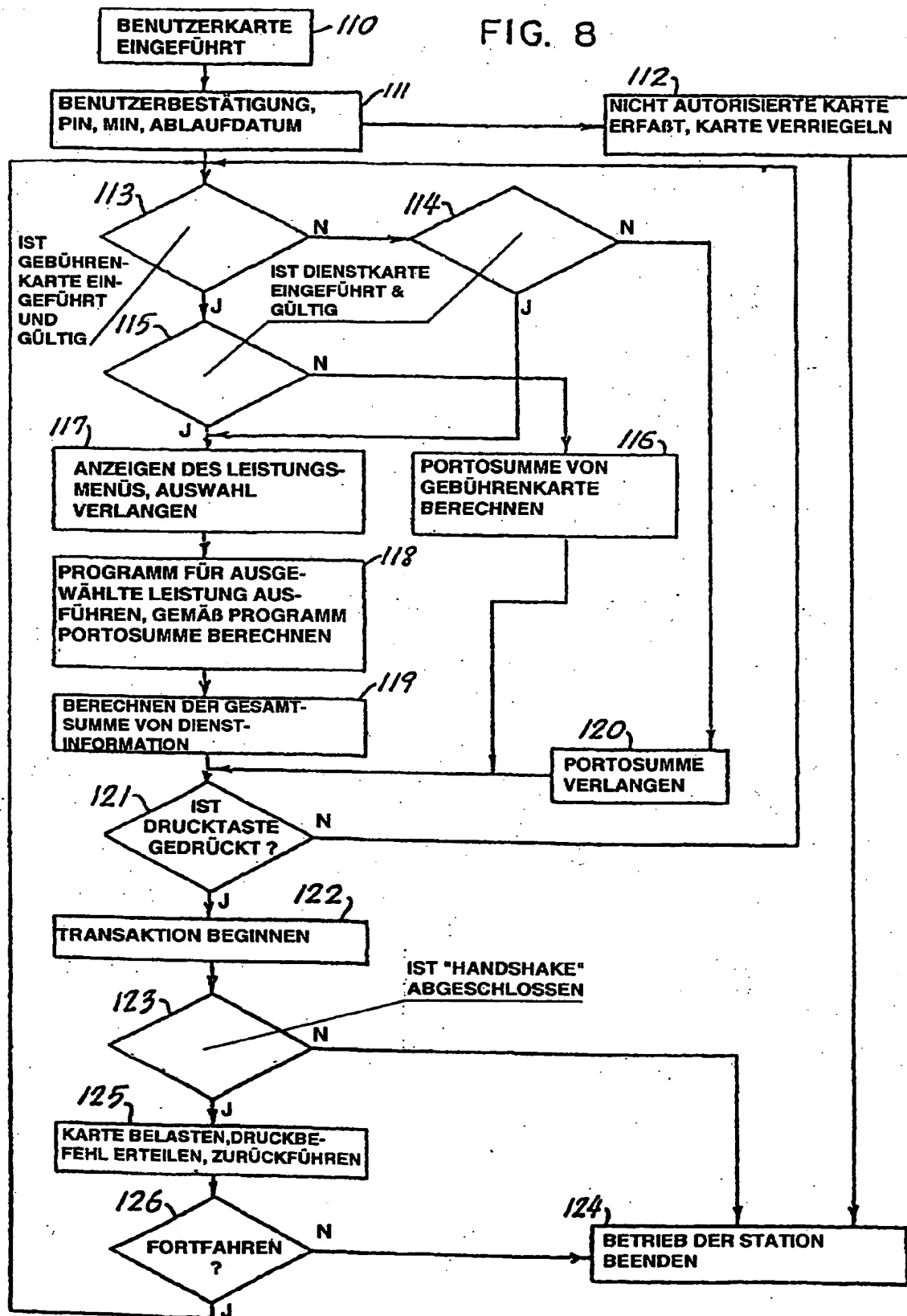


FIG. 7

FIG. 8



27.11.97

9/11

130 U.S. POSTDIENST 138

131 EXPREBPOST

POSTLEITZAHL: 132 AN: 133 DATUM: 134

EINGANGS- ZEIT: 135 GEWICHT: 136

MASCHINE# VON: 137

PORTO: 144 00.00 145

OTHER: 00.00 TO: 141

GESAMT: 00.00

VORAUSSICHTLICHES LIEFERDATUM 142 ZEIT: 143

898926176500

GELIEFERT: 139

140

146

FIG. 9

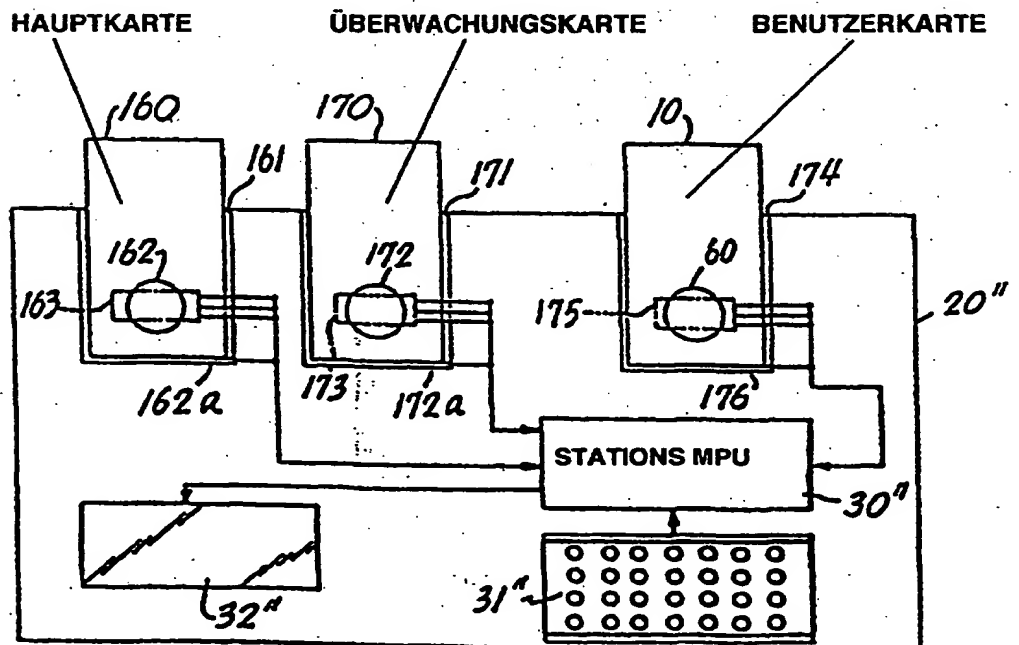


FIG. 10

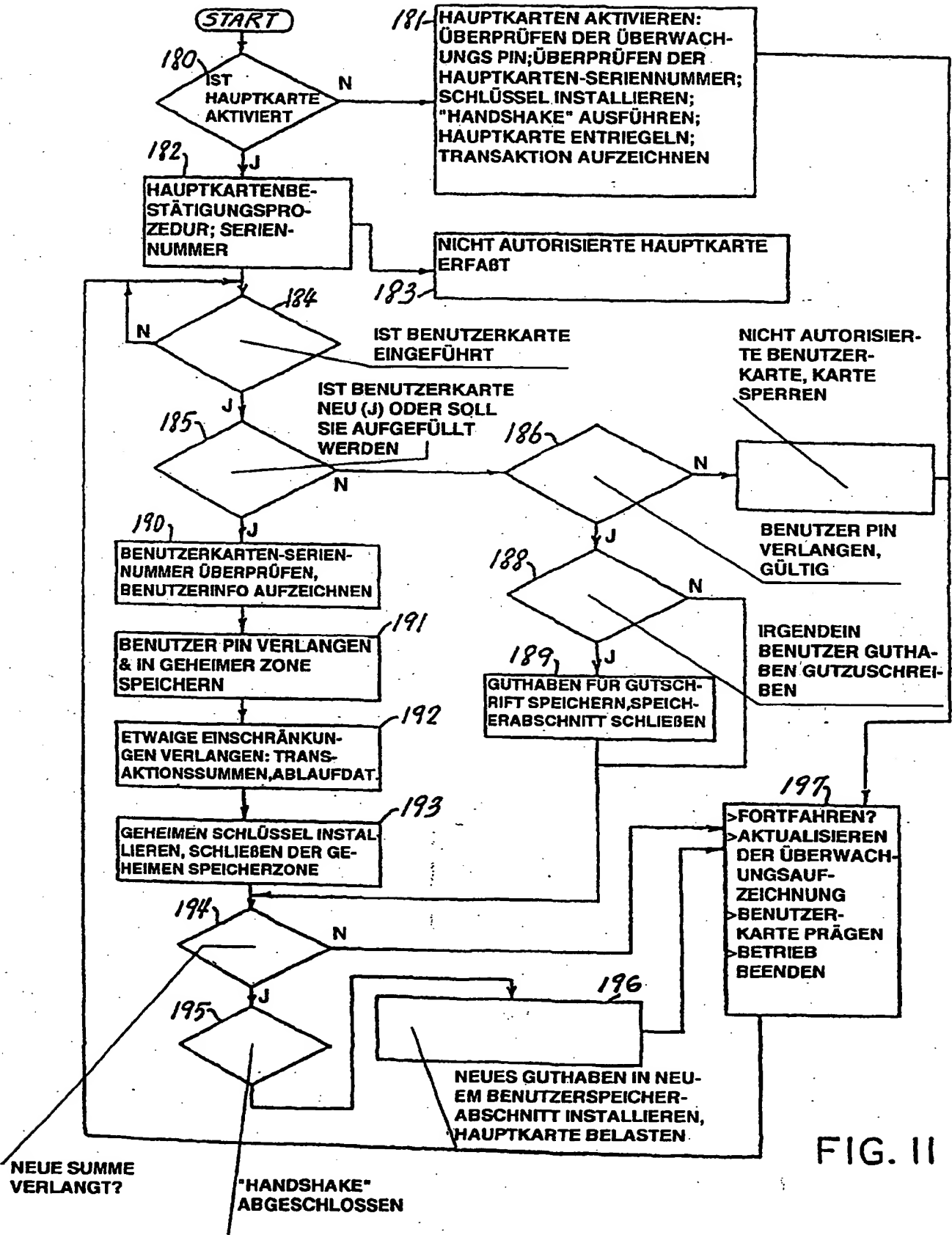


FIG. II

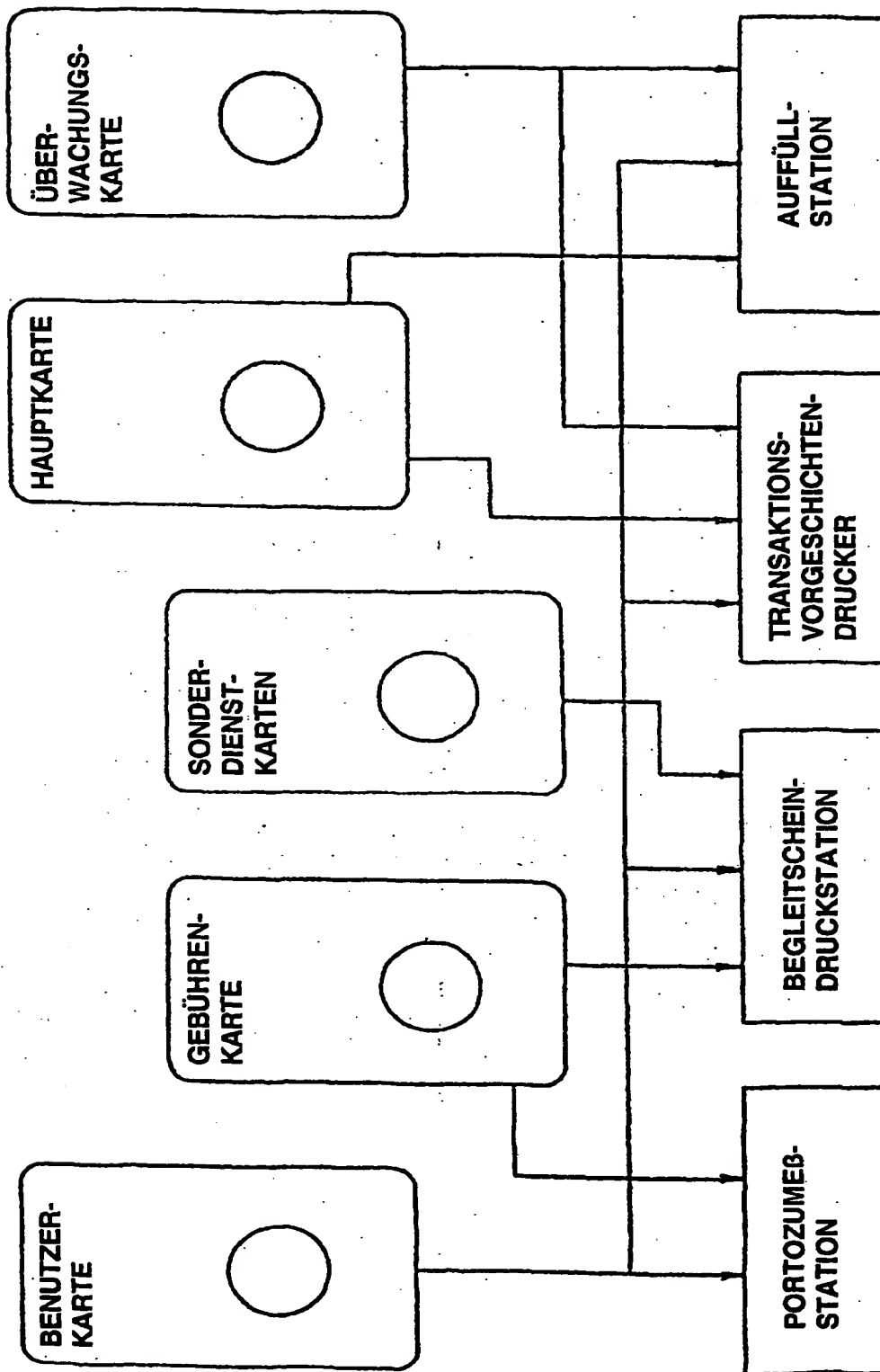


FIG. 12

This Page Blank

This Page Blank (uspto)